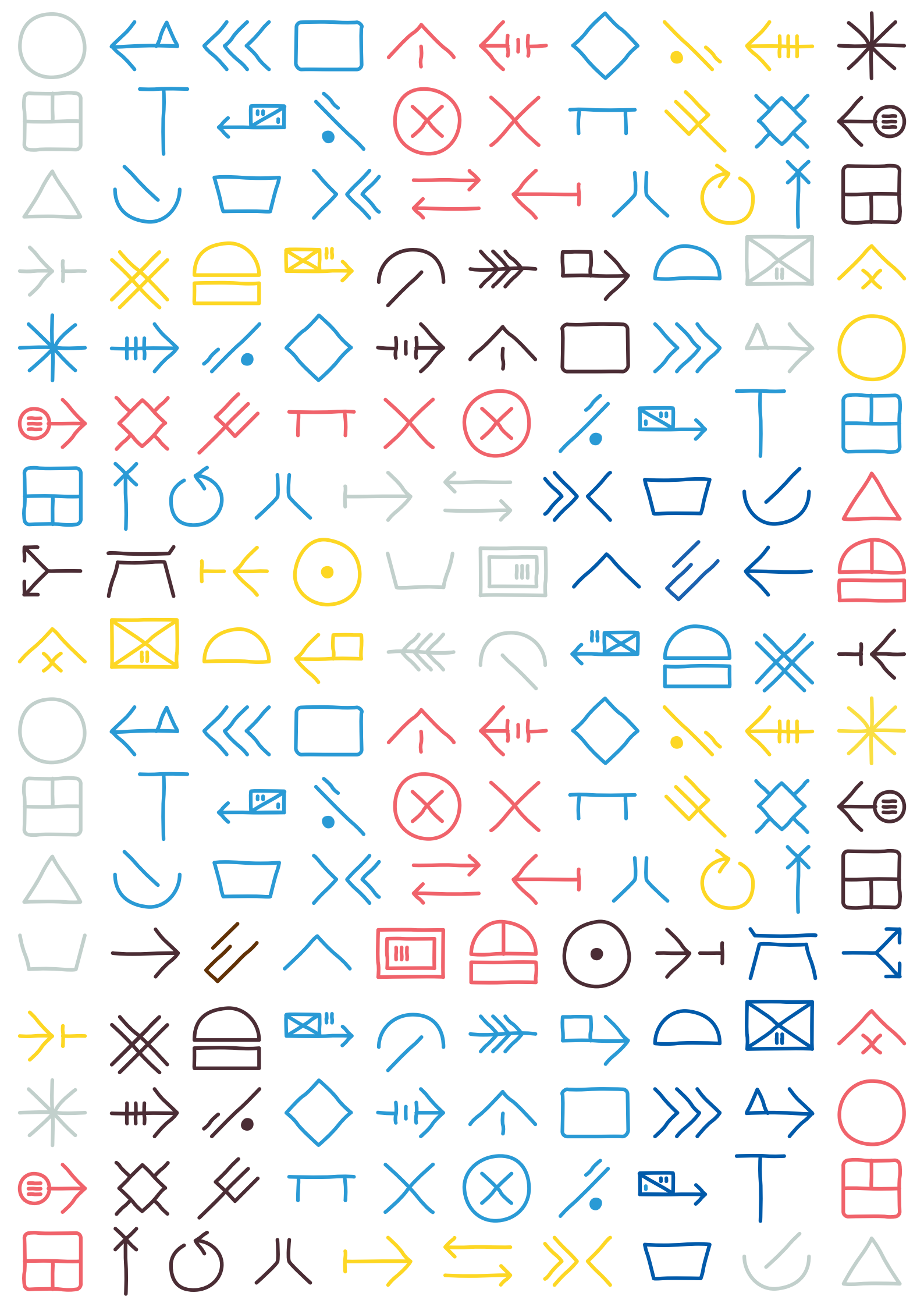
vcp

VERBAND CHRISTLICHER
PFADFINDERINNEN UND
PFADFINDER

Datenschutz im VCP

Informationen für die Arbeit auf Bundes- und Landesebene

* Vorsicht



Inhaltsverzeichnis

Die Grundlagen des Datenschutzes

1

Seit Ende Mai 2018 bekommt der Datenschutz in der öffentlichen Wahrnehmung eine völlig neue Bedeutung. Eine neue, EU-weite Datenschutzgrundverordnung (DSGVO) gilt nun als direkt anwendbares Recht in Deutschland. Angelehnt hieran trat auch das neue Datenschutzgesetz der Evangelischen Kirche in Kraft (DSG-EKD), welches für den VCP als evangelischen Verband Gültigkeit hat.[1] Viel wurde seit dem Inkrafttreten dieser neuen Verordnungen diskutiert. Dabei sind Begriffe wie »Transparenz«, »Recht auf Information« oder auch »Datenminimierung« gefallen. Was sich im ersten Moment wie eine neue Fremdsprache anhört, ist jedoch bei genauerer Betrachtung nicht nur sinnvoll, sondern schützt unsere ureigensten Daten auch im Sinne des Grundgesetzes. Denn hier ist definiert, dass »jede Person […] grundsätzlich das Recht [hat], selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen« (Art. 2 Nr. 1 GG). Datenschutz dient also in erster Linie dem Schutz von Menschen.

§
Art. 2 Nr. 1 GG

Doch was bedeutet Datenschutz genau? Das kann am einfachsten anhand folgender Fragestellungen bestimmt werden (vgl. *Schrock 2018*):

- Was wird geschützt? (Alle personenbezogenen Daten)
- Vor wem? (Hacker*innen, Unternehmen und die eigene Umgebung)
- Für wen? (Menschen – Teilnehmer*innen und Veranstalter*innen)
- Warum? (Demütigung, Verwendung für andere Dinge)
- Wie sicher? (So sicher wie möglich, aber mit vertretbarem Aufwand)
- Wie lange? (Bis Daten für den konkret definierten Zweck nicht mehr benötigt werden)

1.1 Personenbezogene Daten

Datenschutz, wie hier definiert, bezieht sich ausschließlich auf den Schutz personenbezogener Daten von natürlichen Personen. Dies sind alle Daten, die mit einem Menschen in Verbindung gebracht werden können und so eine Identifizierung möglich machen (ebenda (ebd.)).

Zu den personenbezogenen Daten zählen im Sinne des DSG-EKD unter anderem:

1 Im Gegensatz zum VCP-Bundesverband können einzelne VCP-Länder in den Gegenstandsbereich der DSGVO und nicht des DSG-EKD fallen. Dies muss ggf. von den Verantwortlichen der Länder geprüft werden. Beiden Verordnungen bzw. Gesetzen liegen grundsätzlich die gleichen Standards zugrunde, da das kirchliche Datenschutzgesetz der einheitlichen europäischen Datenschutzverordnung angepasst wurde. Gleichzeitig wurden im DSG-EKD jedoch auch Besonderheiten des kirchlichen Datenschutzes berücksichtigt. Regelungen, die nur im DSG-EKD verankert oder, bei denen die DSGVO stark von den hier dargestellten Ausführungen abweicht, sind im Folgenden entsprechend gekennzeichnet.

§
Art. 4 Nr. 1 DSG-EKD

- Name, Anschrift und Geburtsdatum
- E-Mail- und IP-Adresse
- Beruf
- Größe, Gewicht
- Bankverbindung
- Foto- und Filmaufnahmen

Bestimmte Daten sind dabei noch sensibler als andere und deshalb besonders geschützt, da sie zum Beispiel bei Missbrauch der betroffenen Person schaden können (vgl. *Reichmann 2018: 9*). Im Datenschutzrecht werden sie deshalb als »besondere Kategorien personenbezogener Daten« bezeichnet und dürfen nur unter ganz bestimmten Umständen verarbeitet werden. Beispiele für diese Daten sind:

§
Art. 4 Nr. 2 DSG-EKD

- Rassische und ethnische Herkunft
- Informationen zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder zur Gewerkschaftszugehörigkeit (Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft werden im DSG-EKD von dieser Regelung – im Gegensatz zur DSGVO – ausgenommen (Art. 4 Nr. 2 DSG-EKD))
- Genetische oder biometrische Daten, die einen Menschen eindeutig identifizieren
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung
- (Informationen zu strafrechtlichen Daten dürfen nur unter behördlicher Aufsicht verarbeitet werden)

Zur Vereinfachung des Umgangs mit personenbezogenen Daten sollte kein Unterschied zwischen besonders sensiblen und allgemeinen personenbezogenen Daten gemacht, sondern alle Daten gleichwertig geschützt werden.

1.2 Voraussetzungen für die Verarbeitung personenbezogener Daten

§
Art. 4 Nr. 3 DSG-EKD

Grundsätzlich ist die Verarbeitung personenbezogener Daten im geltenden Datenschutzrecht verboten (Art. 4 Nr. 3 DSG-EKD). »Verarbeitung« meint dabei die gesamte Bandbreite dessen, was mit Daten gemacht werden kann: Erhebung, Erfassung, Speicherung, Verbreitung, Verknüpfung, Einschränkung, Löschung und Vernichtung – also letztendlich jede Form der Verwendung und Nutzung personenbezogener Daten.

Es existieren jedoch Ausnahmen von diesem Verbot, etwa der sogenannte »Erlaubnisvorbehalt« (Art. 6 DSG-EKD). Dieser ist durch das Daten-

schutzrecht genau definiert und geregelt. Daten dürfen nur dann verarbeitet werden, wenn

§
Art. 6 Nr. 1–8 DSG-EKD

- die Einwilligung der betroffenen Person vorliegt.
  Bei Kindern und Jugendlichen müssen die Erziehungsberechtigten in der Regel mitzustimmen. Eine Ausnahme bilden dabei nach § 12 DSG-EKD elektronische Angebote, für welche die*der Jugendliche zur selbstständigen Einwilligung die »Religionsmündigkeit« – das vollendete vierzehnte Lebensjahr – erreicht haben muss.[2]

- ein »überwiegend berechtigtes Interesse« besteht.
  Der VCP hat beispielsweise ein berechtigtes Interesse daran, Daten seiner Mitglieder zu verarbeiten, wenn dies für die Beantragung von Zuschüssen und Förderungen notwendig ist.

- die Daten zur Vertragserfüllung notwendig sind.
  Die personenbezogenen Daten, welche für die Vertragserfüllung notwendig sind, ergeben sich aus dem Vereinszweck, der in der Satzung festgelegt ist. Dies ist im VCP unter anderem das Alter eines Mitglieds, um zielgruppengerechte Pfadfinder*innenarbeit zu gewährleisten.

- es um Leben und Tod geht.
  Hierzu gehören beispielsweise lebensgefährliche Allergien bei Teilnehmer*innen einer Veranstaltung.

- eine gesetzliche Verpflichtung herrscht.
  Dies umfasst beispielsweise Daten für Steuerbehörden oder für die Rentenversicherung bei hauptberuflichen Mitarbeiter*innen, aber auch personenbezogene Daten, die zur Wahrnehmung der Aufsichtspflicht bei Veranstaltungen notwendig sind.

- es sich um anonyme Daten handelt, die frei verfügbar sind.
  Da es sich bei anonymen Daten, also Daten, die unter keinem Umstand einer Person zugeordnet werden können, nicht mehr um personenbezogene Daten handelt. Dazu gehören beispielsweise Daten aus statistischen Erhebungen.

Die wohl wichtigste Ausnahme vom allgemeinen Verbotsprinzip für die Arbeit im VCP ist die aktive Einwilligung einer betroffenen Person zur Datenverarbeitung. Hierbei ist die Schriftform zwar nicht mehr in allen Fällen notwendig, erleichtert jedoch später die Beweisführung und wird daher empfohlen (vgl. *Schrock 2018*). Zwingend vorgeschrieben ist eine schriftliche Einwilligung hingegen bei der Verarbeitung von besonderen

2 Für den Geltungsbereich der DSGVO muss bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind/einer*einem Jugendlichen direkt gemacht wird, ein*e Minderjährige*r zur Einwilligung das sechzehnte Lebensjahr vollendet haben (Art. 8 Nr. 1 DSGVO).

Kategorien personenbezogener Daten. Eine solche Erklärung zur Einwilligung in die Datenverarbeitung muss umfassend informieren, warum diese Daten erhoben und wofür sie benötigt werden, was genau mit diesen Daten gemacht wird und auch, welche Rechte betroffene Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten haben. Dabei sollen sie in leicht zugänglicher Form sowie in einer klaren und einfach zu verstehenden Sprache vorliegen, so dass die Erklärung von anderen Sachverhalten eindeutig zu unterscheiden ist (ebd.).

1.3 Grundsätze bei der Verarbeitung personenbezogener Daten

Die gelisteten Ausnahmen – oder auch Erlaubnisvorbehalte – erlauben die Verarbeitung personenbezogener Daten. Dies bedeutet jedoch keineswegs, dass personenbezogene Daten für alles und in jeder Form verwendet werden dürfen. Klar definierte Grundsätze, die immer eingehalten werden müssen, regeln den Umgang mit personenbezogenen Daten:

§
Art. 5 Nr. 1 DSG-EKD

- ***Transparenz*** (Art. 5 Nr. 1 DSG-EKD): Die Datenverarbeitung muss transparent erfolgen. Betroffene Personen müssen darüber in Kenntnis gesetzt werden, wie ihre personenbezogenen Daten verarbeitet werden (ebd.). Dabei müssen sie in leichter Sprache und einfach zugänglich informiert werden, was die Verarbeitung ihrer Daten umfasst, wer diese Daten verwendet und wohin sie ggf. übertragen werden (ebd.). Betroffene Personen müssen aber auch verstehen, wo die Grenzen der Verarbeitung liegen (ebd.). Dies bedeutet, dass alle Verarbeitungsschritte deshalb bereits vor Beginn der Datenverarbeitung geklärt und dokumentiert sein müssen (ebd.).

- ***Zweckbindung*** (Art. 5 Nr. 1 DSG-EKD): Die Einwilligung in die Datenverarbeitung ist an einen bestimmten Zweck gebunden. Für zusätzliche oder neue Nutzungszwecke für bereits erhobene Daten muss eine erneute, explizite Zustimmung der betroffenen Person eingeholt werden (ebd.). Ein Beispiel hierfür wäre, dass Daten, die für den Zweck eines Stammeslagers erhoben wurden, nur mit erneuter Zustimmung des Mitglieds für die Teilnahme an einer Aussendungsfeier für das Friedenslicht benutzt werden dürfen.

- ***Richtigkeit*** (Art. 5 Nr. 1 DSG-EKD): Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Dabei sind alle angemessenen Maßnahmen zu treffen, damit Daten, die im Hinblick auf ihren Verarbeitungszweck unrichtig sind, unverzüglich berichtigt oder gelöscht werden. Dies bedeutet beispielsweise, wenn eine Person eine neue Kontaktadresse meldet, muss die alte unverzüglich gelöscht und durch die richtige ersetzt werden.

- ***Datenminimierung*** (Art. 5 Nr. 1 DSG-EKD): Es dürfen nur solche Daten erhoben werden, die auch für die vorher festgelegten, eindeutigen und legitimen Zwecke gebraucht werden (vgl. *Schrock 2018*). Der Grundsatz heißt hierbei: »So wenig wie nötig«.

- ***Speicherbegrenzung*** (Art. 5 Nr. 1 DSG-EKD): Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie für die Zwecke, für die sie verarbeitet werden, erforderlich sind. Wenn beispielsweise ein Lager beendet ist, müssen Daten zu den Essensgewohnheiten der Teilnehmer*innen gelöscht werden.

- ***Integrität und Vertraulichkeit*** (Art. 5 Nr. 1 DSG-EKD): Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung ein. Daten müssen sicher aufbewahrt werden und es muss sichergestellt sein, dass nur Personen, die diese personenbezogenen Daten wirklich brauchen, auch Zugriff haben. Hierfür müssen geeignete technische und organisatorische Maßnahmen getroffen werden. Zum Beispiel benötigen Leitungen von Zeltlagern die Daten der Teilnehmer*innen. Umgekehrt ist dies aber nicht notwendig (vgl. *Reichmann 2018: 13*).

- ***Treu und Glauben*** (Art. 5 Nr. 1 DSG-EKD): Daten dürfen nicht heimlich und ohne Zustimmung der betroffenen Person erhoben und verarbeitet werden. Hierzu gehören beispielsweise unerlaubte Handy-Aufnahmen während geschlossener Sitzungen (vgl. *Reichmann 2018: 11*).

- ***Rechenschaftspflicht*** (Art. 5 Nr. 2 DSG-EKD): Die verantwortliche Stelle für die Verarbeitung personenbezogener Daten muss die Einhaltung dieser Grundsätze nachweisen können. Dies bedeutet beispielsweise, dass Lagerleitungen, die ein Landeslager organisieren, oder auch hauptberufliche Referent*innen, die eine Schulung anbieten, nachweisen können müssen, dass die Grundätze des Datenschutzes eingehalten werden. Eine Ausnahme besteht, wenn diese Personen im Auftrag eines Vorstands oder anderer Leitungen handeln. Dann liegt die Verantwortung bei den Vorständen/Leitungen.

§
Art. 5 Nr. 2 DSG-EKD

- ***Meldepflicht*** (Art. 32 DSG-EKD): Sollten personenbezogene Daten verloren gehen und dadurch ein Schaden für eine natürliche Person auftreten, besteht eine Meldepflicht. Hierbei muss eine unverzügliche Meldung (das heißt, eine Meldung ohne schuldhaftes Verzögern – in der Regel binnen 72 Stunden) bei der zuständigen Datenschutzbehörde erfolgen.

§
Art. 32 DSG-EKD

- ***Privacy by Design/Privacy by Default:*** Einstellungen bei Softwareprogrammen müssen so gestaltet sein, dass die Nutzer*innendaten

standardmäßig bestmöglich geschützt sind. So dürfen nur die Daten in den Voreinstellungen abgefragt werden, die unbedingt notwendig sind.

§
Art. 20 DSG-EKD

- ***Recht auf Berichtigung und Vollständigkeit*** (Art. 20 DSG-EKD): Betroffene Personen haben das Recht darauf, dass ggf. falsche Daten berichtigt werden und unvollständige Daten, insbesondere, wenn sie aufgrund ihrer Unvollständigkeit ein falsches Bild der betroffenen Person vermitteln, ergänzt werden (vgl. *Weller 2020: 61*).

§
Art. 11 DSG-EKD

- ***Recht auf Widerruf*** (Art. 11 DSG-EKD): Eine betroffene Person hat das Recht, ihre ursprüngliche Einwilligung zur Datenverarbeitung zu widerrufen. Dies ist ohne Nennung von Gründen möglich. Wenn die Grundlage einer Datenvereinbarung rein auf dem Erlaubnisvorbehalt der »Einwilligung« und keiner weiteren Ausnahme beruht, müssen die personenbezogenen Daten gelöscht werden. Dabei hat ein Widerruf jedoch erst mit Blick auf zukünftige, verarbeitende Tätigkeiten Bestand. Die Datenverarbeitung bis zum Zeitpunkt des Widerrufs bleibt rechtmäßig.

§
Art. 25 DSG-EKD

- ***Recht auf Widerspruch*** (Art. 25 DSG-EKD): Auch hat eine betroffene Person das Recht, Widerspruch gemäß Art. 25 DSG-EKD einzulegen. Dieser muss begründet sein durch eine »besondere Situation«, die gegen die Verarbeitung ihrer personenbezogenen Daten spricht; das heißt es müssen besondere, nachvollziehbare Gründe gegen die Datenverarbeitung vorliegen (vgl. *Weller 2020: 63*). Dabei gilt, dass die Interessen des Verbands gegenüber den Interessen der betroffenen Person abzuwiegen sind. Überwiegt die Schutzbedürftigkeit der betroffenen Person, insbesondere in Bezug auf ihr Recht auf Privatsphäre, dürfen die Daten nicht mehr verarbeitet, sondern müssen gelöscht werden (vgl. *Weller 2020: 64*).

§
Art. 21 DSG-EKD

- ***Recht auf Vergessenwerden*** (Art. 21 DSG-EKD): Betroffene haben das Recht, dass nicht mehr für den ursprünglichen Zweck notwendige und nicht mehr genutzte Daten aktiv gelöscht werden. Dabei müssen zur Datenvernichtung geeignete technische und organisatorische Maßnahmen ergriffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[3] Obwohl hierbei keine festen Fristen festge-

3 Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung. Dieses ist jedoch nur im kirchlichen Datenschutzrecht (Art. 22 DSG-EKD) verankert. Es besagt, dass personenbezogene Daten zwar noch gespeichert werden dürfen, ihre Verarbeitung jedoch nur mit ausdrücklicher Einwilligung der betroffenen Person zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person verarbeitet werden dürfen.

legt sind, sollte die Löschung so schnell wie möglich unter Abwägung der Interessen der beteiligten Parteien erfolgen. Das »Recht auf Vergessenwerden« ist jedoch nicht allumfassend. Gründe, die das Recht auf Löschung außer Kraft setzen, werden in Art. 21 Nr. 3 des DSG-EKD gelistet. Diese Gründe gelten auch, wenn Widerspruch eingelegt oder eine Einverständniserklärung widerrufen wurde:

§
Art. 21 Nr. 3 DSG-EKD

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
- zur Erfüllung einer rechtlichen Verpflichtung, welcher die verantwortliche Stelle unterliegt,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- zur Wahrnehmung einer Aufgabe, die im kirchlichen (DSGVO: öffentlichen) Interesse liegt oder in Ausübung hoheitlicher (DSGVO: öffentlicher) Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde,
- für im kirchlichem (DSGVO: öffentlichen) Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, wenn das Löschen der Daten dies unmöglich macht oder ernsthaft verhindert,
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- und, wenn einer Löschung satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

Zusammenfassend ist festzuhalten, dass der Datenschutz grundsätzlich dem Schutz unserer persönlichen Daten und damit dem Schutz von Menschen dient. Deswegen gilt für personenbezogene Daten ein generelles Verarbeitungsverbot, das nur in bestimmten Ausnahmefällen aufgehoben werden kann. Die Grundsätze der Datenverarbeitung regeln dabei, wie mit diesen Daten umgegangen werden muss und welche Rechte die betroffenen Personen haben.

1.4 Dokumentation von Verarbeitungstätigkeiten

Um festzuhalten, wie ein Verband oder Verein mit personenbezogenen Daten umgeht, muss er den Status quo darlegen. Dieses sogenannte Verzeichnis von Verarbeitungstätigkeiten ist ein schriftliches oder elektronisches, internes Verzeichnis, das auf Anfrage der zuständigen Aufsichtsbehörde für den Datenschutz vorzulegen ist (vgl. *Art. 31 Nr. 1–4 DSG-EKD*).

§
Art. 31 DSG-EKD

Diese allgemeine Pflicht gilt nur für Vereine mit mehr als 250 (haupt- oder ehrenamtlichen) Mitarbeiter*innen. So sind der VCP und seine Unterglie-

derungen vom Führen eines Verzeichnisses für alle personenbezogenen Daten befreit. Aber Vorsicht, unabhängig hiervon sind in jedem Fall und ohne Ausnahme die Verfahren im Umgang mit besonderen Kategorien personenbezogener Daten zu dokumentieren (siehe Kapitel 1.1). Im VCP sind dies beispielsweise Gesundheitsdaten wie Allergien oder Krankheiten, die eine Medikamentierung benötigen und im Rahmen eines Lagers von den Teilnehmer*innen zur Verfügung gestellt werden.[4] Das Muster für ein solches Verarbeitungsverzeichnis für diese Datenkategorie auf Grundlage des Datenschutzgesetzes der Evangelischen Kirche ist unter *https://datenschutz.ekd.de/infothek-items/verzeichnis-der-verarbeitungstaetigkeiten* abrufbar.

Praxistipp Corona-Pandemie: Bei Veranstaltungen und Aktionen muss der*die Veranstalter*in im Rahmen des Infektionsschutzgesetzes Name, Anschrift und Telefonnummer der Teilnehmer*innen zur Ermöglichung der Nachverfolgung von Infektionsketten erfassen (vgl. *Weller 2020: 71*). Datenschutzrechtlich ist dies durch den Schutz lebenswichtiger Interessen in Art. 6 Nr. 7 DSG-EKD abgedeckt. Die Daten sind geschützt vor dem Zugriff Dritter aufzubewahren, für zuständige Behörden (zum Beispiel das Gesundheitsamt) aufzuheben und auf Anforderung an diese weiterzugeben (ebd.). Nach Ablauf der gesetzlichen Frist, in der Regel ein Monat, müssen die Daten unverzüglich gelöscht werden.

1.5 Verarbeitung von personenbezogenen Daten durch externe Dienstleister*innen

Personenbezogene Daten werden nicht nur innerhalb des Verbands verarbeitet. Oft werden externe Dienstleister*innen mit beispielsweise der Betreuung der Mitgliederdatenbank oder der Webseite beauftragt. Aber auch Versandanbieter, die Zeitungen oder Newsletter im Auftrag des VCP versenden, verarbeiten personenbezogene Daten. Hierbei gibt also der Verband personenbezogene Daten an Dritte oder Unternehmen weiter, gewährt die Abfrage weiterer Daten und/oder gibt Daten zu einem bestimmten Zweck ab (vgl. *Weller 2020: 77*). Im Sinne des Datenschutzrechtes ist dies eine Auftragsverarbeitung. Sie ist definiert als Verarbeitung von personenbezogenen Daten durch eine*n Auftragnehmer*in (Auftrags-

4 Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft sind im DSG-EKD nicht Bestandteil der besonderen Kategorien personenbezogener Daten. Für VCP-Länder, die in den Geltungsbereich der DSGVO fallen, müssen diese Angaben in ein Verarbeitungsverzeichnis aufgenommen werden.

verarbeiter*in) auf Anordnung der*des Auftraggeberin*Auftraggebers (hier: der VCP) auf Grundlage eines schriftlichen Vertrags (ebd.). Trotz dieser »Auslagerung« der datenverarbeitenden Tätigkeiten bleibt jedoch der VCP für die Einhaltung des Datenschutzrechtes weiterhin verantwortlich und hat auch in Bezug auf dieses das Weisungs- und Kontrollrecht (vgl. *Art. 30 Nr. 1 DSG-EKD*; vgl. *Weller 2020: 77*). Daher muss der*die Auftragsverarbeiter*in sorgfältig ausgewählt werden. Es ist genau zu prüfen, welche Vorkehrungen und Garantien er*sie für die Sicherstellung des Datenschutzes trifft (ebd.). Wenn die Auswahl des*der Auftragsverarbeitenden nicht nachweislich mit Sorgfalt geschieht, kann ein sogenanntes »Auswahlverschulden« vorliegen (ebd.).

§
Art. 30 DSG-EKD

Nach Artikel 30 des DSG-EKD muss ein geschlossener Auftragsverarbeitungsvertrag auf alle Fälle den Gegenstand und die Dauer des Auftrags sowie den Umfang, die Art und den Zweck der Verarbeitung beinhalten. Zusätzlich ist festzulegen, welche Art der Daten überhaupt verarbeitet werden und um wessen Daten es sich dabei handelt. Wichtig ist außerdem, dass die Weisungsbefugnisse des Verbands klar geregelt sind, im Vertrag eine Verpflichtung auf Vertraulichkeit enthalten ist und eine Gewährleistung der technischen und organisatorischen Sicherheit der Datenvereinbarung dargestellt wird (ebd.). Für den Fall der Beendigung des Vertragsverhältnisses muss eine Klausel eingefügt sein, welche die Rückgabe und Löschung von Daten beinhaltet (ebd.). Die Einhaltung dieser Vorgaben seitens des*der Auftragsverarbeiters*Auftragsverarbeiterin ist durch den Verband regelmäßig zu überprüfen und zu dokumentieren. Sofern die kirchlichen Datenschutzbestimmungen auf den*die Auftragsverarbeiter*in nicht zutreffen (keine Anwendung des DSG-EKD), ist der Verband verpflichtet, sicherzustellen, dass der*die Auftragsverarbeiter*in diese oder gleichwertige Bestimmungen beachtet (vgl. *Art. 30 Nr. 5 DSG-EKD*). In diesem Fall darf der Vertrag auch auf Grundlage des Art. 28 der DSGVO geschlossen werden. Der*Die Auftragsverarbeiter*in unterwirft sich jedoch damit der kirchlichen Datenschutzaufsicht.[5] Vorlagen für den AV-Vertrag und die eventuell notwendige Zusatzvereinbarung können unter *https://datenschutz.ekd.de/infothek-items/av-vertrag/*abgerufen werden.

Diese Regelung gilt nicht nur für langfristig ausgelegte Dienstleistungen. Auch mit temporären Dienstleister*innen, welche Leistungen im Rahmen von digitalen Versammlungen erbringen, muss unter Umständen ein Auftragsverarbeitungsvertrag abgeschlossen werden. Dabei ist zu unterscheiden, ob nur eine Plattform zur Verfügung gestellt wird und die Dienstleister*innen nicht in Kontakt mit personenbezogenen Daten der Teilnehmer*innen (IP-Adresse, Name, Profilbild etc.) kommen oder diese Daten auch für die externen Dienstleister*innen ersichtlich sind (vgl. *Weller 2020: 77*). Dies ist etwa der Fall, wenn sie während einer Veranstaltung auch technische Unterstützung für die Teilnehmer*innen leisten.

5 Für VCP-Länder, die unter die DSGVO fallen, entfällt diese Regelung.

Sobald personenbezogene Daten einsehbar sind, muss ein Auftragsverarbeitungsvertrag abgeschlossen werden (ebd.).

Eine Ausnahme von diesen Regelungen zur Auftragsverarbeitung sind Verträge mit Rechtsanwält*innen, Steuerberater*innen und Geldinstituten. Hierbei handelt es sich um die sogenannte »Inanspruchnahme fremder Fachleistungen bei einem eigenständigen Verantwortlichen« *(*vgl. *Weller 2020: 78*). Sie arbeiten selbstständig, sind weisungsunabhängig und eigenverantwortlich tätig, was der Weisungsgebundenheit, wie sie im DSG-EKD festgelegt ist, widerspricht und sie somit nicht unter die aufgeführten Regelungen fallen lässt (ebd.).

Bei Abschluss eines Vertrags mit einem*einer Dienstleister*in wird in der Regel automatisch ein AV-Vertrag durch den*die Dienstleister*in zur Kenntnisnahme und Unterschrift bereitgestellt. Dieser muss jedoch unbedingt auf oben genannte Punkte überprüft werden.

Die*Der örtliche Beauftragte für den Datenschutz

2

Die*Der örtlich Beauftragte für den Datenschutz (ehemals Datenschutzbeauftragte*r; kurz: öBD) in einem Kinder- und Jugendverband sind die Personen, die für die Umsetzung des Datenschutzes vor Ort zuständig sind (vgl. *Weller 2020: 85*). Damit sie diese Aufgabe auch erfüllen können, hat die DSGVO und auch das DSG-EKD sie mit vielen Befugnissen, aber auch Pflichten ausgestattet (ebd.). Dabei hat der*die örtlich Beauftragte für den Datenschutz nicht nur eine Kontrollaufgabe, sondern soll auch auf den richtigen und rechtskonformen Umgang mit personenbezogenen Daten vorab aufmerksam machen (ebd.). Dafür ist die Zusammenarbeit zwischen Leitung, hauptberuflichen Mitarbeiter*innen, VCP-Mitgliedern und öBD entscheidend für die nachhaltige Umsetzung des Datenschutzes.

2.1 Notwendigkeit einer*eines örtlich Beauftragten für den Datenschutz

Die Frage, ob ein*e örtlich Beauftragte*r für den Datenschutz notwendig ist, ist im Datenschutzgesetz der Evangelischen Kirche durch die magische Zahl »10« geregelt. Sind in der Regel ständig mindestens zehn Personen mit der Verarbeitung personenbezogener Daten betraut, oder aber, wenn die Kernarbeit der verantwortlichen Stelle aus der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht, muss ein*e örtlich Beauftragte*r für den Datenschutz bestellt werden (vgl. *Kamm 2020*).[6]

Im Sinne des Datenschutzes zählen zum Personenkreis, welcher mit der Ermittlung und Verarbeitung personenbezogener Daten betraut ist, sämtliche Personen, die im Auftrag eines Vereins oder Verbands Leistungen erbringen (ebd.). Dabei spielt es keine Rolle, ob diese Tätigkeit im Rahmen einer bezahlten Anstellung oder eines ehrenamtlichen Engagements ausgeübt wird.

Eine »ständige Beschäftigung« mit personenbezogenen Daten liegt dann vor, wenn diese über einen längeren Zeitraum wahrgenommen wird (vgl. *Weller 2020: 86*). Im VCP betrifft dies typischerweise die Mitgliederverwaltung über eVEWA, den Betrieb eines E-Mail-Verteilers, den Versand von regelmäßigen Newslettern, Einladungen zu Veranstaltungen etc.

Rechtlich sind dabei sämtliche Gliederungen – unabhängig von ihrer eigenen Rechtsform (eingetragener Verein, Teil des Gesamtverbands etc.) –

6 Für nicht-kirchliche Stellen ist die Notwendigkeit eines*einer örtlich Beauftragten für den Datenschutz in Art. 38 des Bundesdatenschutzgesetzes geregelt. Dieser besagt, dass ein*e öBD notwendig ist, soweit in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

§
Art. 36 Nr. 1 DSG-EKD

beim Vorliegen dieser Voraussetzungen nach Art. 36 Abs. 1 des DSG-EKD zur Bestellung einer*eines örtlichen Beauftragten für den Datenschutz verpflichtet (vgl. *Kamm 2020*). Diese Verpflichtung wird jedoch aufgehoben, wenn sie weisungsgebundener Teil einer anderen Gliederung sind; also nicht eigenständig über die Verarbeitung von personenbezogenen Daten entscheiden können (ebd.).

Umfasst der Personenkreis, der regelmäßig oder umfangreich personenbezogene Daten in einer Gliederung des VCP verarbeitet bzw. Einsicht hierauf hat, mehr als 10 Personen, so ist ein*e örtlich Beauftragte*r für den Datenschutz zu bestellen.

2.2 Voraussetzungen einer*eines örtlich Beauftragten für den Datenschutz

Die Aufgaben einer*eines örtlich Beauftragten für den Datenschutz sind vielfältig, anspruchsvoll und bedeutsam. Deswegen hat die Gesetzgebung bestimmt, dass hierfür besondere Qualifikationen notwendig sind.

§
Art. 36 Nr. 3–5 DSG-EKD

Im DSG-EKD sind diese unter Art. 36 Nr. 3–5 wie folgt festgelegt:

- *(3) Zu örtlich Beauftragten dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Die Bestellung kann befristet für mindestens drei Jahre erfolgen.*
  Dies bedeutet, dass örtlich Beauftragte für den Datenschutz das geltende Datenschutzrecht kennen, technische Kenntnisse in der Datenschutzpraxis besitzen sowie vertieftes Wissen über die individuellen Gegebenheiten des Vereins oder Verbands haben oder sich aneignen müssen (vgl. *Weller 2020: 92*). Zur Erlangung und zur Erhaltung dieses Fachwissens müssen dem*der öBD die Teilnahme an Fort- und Weiterbildungsveranstaltungen sowie die Anschaffung von Fachbüchern ermöglicht und die Kosten hierfür getragen werden (vgl. *Art. 37 Nr. 3 DSG-EKD*).

- *(4) Zu örtlich Beauftragten sollen diejenigen nicht bestellt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung der kirchlichen Stelle obliegt.*[7]
  Die*Der örtlich Beauftragte für den Datenschutz ist unabhängig und berichtet unmittelbar der obersten Ebene der jeweiligen Gliederung eines Verbands oder Vereins. Deshalb kann sie*er nicht auch selbst

7 Analog Art. 38 DSGVO: Da der*die öDB unmittelbar der höchsten Managementebene der jeweiligen Gliederung berichtet, kann er*sie nicht mit dieser identisch sein.

gleichzeitig Teil dieser Ebene sein und sich so selbst in Bezug auf den Datenschutz kontrollieren (vgl. *Weller 2020: 93*).

- *(5) Die Bestellung von örtlich Beauftragten erfolgt schriftlich und ist der Aufsichtsbehörde und der nach dem jeweiligen Recht für die allgemeine Aufsicht zuständigen Stelle anzuzeigen; die Kontaktdaten sind zu veröffentlichen.*
  Über die Bestellung einer*eines örtlich Beauftragten für den Datenschutz und dessen*deren Kontaktinformationen sollten, neben der zuständigen Aufsichtsbehörde,[8] möglichst viele Mitglieder des Verbands/Vereins informiert werden. Dabei sollten auch unterschiedliche Kommunikationskanäle genutzt werden, so dass alle die Möglichkeit haben, dies zu sehen, zu registrieren und sich bei Fragen an ihn*sie zu wenden.

Faktisch werden die meisten VCP-Stämme und Gruppen die rechtliche Notwendigkeit für die Bereitstellung einer*eines örtlich Beauftragten für den Datenschutz nicht erfüllen (vgl. *Kamm 2020*). Diese besagt, dass eine Beauftragung nur dann ausgesprochen werden muss, wenn in der jeweiligen Stelle in einem bestimmten Umfang oder einer bestimmten Intensität personenbezogene Daten durch mindestens zehn Personen ständig verarbeitet werden.

8 Die unabhängige Aufsichtsbehörde für den kirchlichen Datenschutz ist der*die Beauftragte für den Datenschutz der EKD. Die Kontrolle über die Stellen, die der DSGVO unterliegen, haben hingegen die Landesdatenschutzbeauftragten.

Datenschutz im Jugendverband

3

Das geltende Datenschutzrecht ist für alle öffentlichen Einrichtungen, Unternehmen und auch für Jugendverbände wie den VCP rechtlich bindend. Besonderheiten bei der Art der personenbezogenen Daten und dem Alter der betroffenen Personen machen es jedoch sinnvoll, die Prozesse, die im VCP am häufigsten vorkommen, detaillierter zu betrachten. Die folgenden Ausführungen stellen daher eine Auswahl, jedoch keine abschließende Auflistung dieser Prozesse dar. Bei weiterführenden Fragen oder Anmerkungen steht der örtlich Beauftragte für den Datenschutz der Bundesebene, Tobias Schwick, unter *datenschutz@vcp.de* zu Verfügung.

3.1 Minderjährige im Datenschutzrecht

In einem Kinder- und Jugendverband ist insbesondere die Frage nach den Datenschutzrechten von Minderjährigen wichtig. Während im alten Datenschutzrecht keine Regelung existierte, erkennt die DSGVO und auch das DSG-EKD an, dass auch Kinder und Jugendliche bei der Verarbeitung ihrer personenbezogenen Daten mitbestimmen sollten (vgl. *Schrock 2020*). Minderjährige dürfen laut geltendem Datenschutzrecht dann selbst einwilligen, wenn sie in der Lage sind, die Auswirkungen ihrer Einwilligung und damit der Verwendung ihrer Daten einzuschätzen (vgl. *Weller 2020: 54*). Ob jedoch dieses Einschätzungsvermögen vorhanden ist, kann von den verantwortlichen Personen für den Datenschutz in den meisten Fällen nicht zweifelsfrei festgestellt werden (ebd.). Zudem können die Erziehungsberechtigten des Kindes oder der*des Jugendlichen auch noch im Nachhinein der Zustimmung ihrer*ihres Schutzbefohlenen widersprechen (ebd.). Um daher sicherzugehen, dass die Interessen und Rechte aller beteiligten Personen bei der Verarbeitung von Daten Minderjähriger gewahrt werden, sollten Erziehungsberechtigte und das Kind bzw. der*die Jugendliche gemeinsam zustimmen. Denn während Minderjährige evtl. nicht abschätzen können, wie weitreichend ihre datenschutzrechtliche Einwilligung ist, ist die umgekehrte Erkenntnis, etwas nicht zu wollen, deutlich früher vorhanden (vgl. *Kamm 2020*). Für Datenverarbeiter*innen bedeutet dies, dass grundsätzlich mit vertretbarem Aufwand zu überprüfen ist, ob eine vorliegende Einwilligung rechtmäßig ist.

§
Art. 12 DSG-EKD

Mit Verweis auf elektronische Angebote bzw. »Dienste der Informationsgesellschaft« wird im Datenschutzrecht der Evangelischen Kirche die Einwilligungsfähigkeit mit der Religionsmündigkeit – also ab 14 Jahren – erreicht (Art. 12 DSG-EKD).[9] Unter diese Regelung fallen Dienstleistungen, die regelmäßig gegen Entgelt, elektronisch, im Fernabsatz und auf indi-

9 Für den Geltungsbereich der DSGVO muss bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind bzw. einem*einer Jugendlichen direkt gemacht wird, ein*e Minderjährige*r zur Einwilligung das sechzehnte Lebensjahr vollendet haben (Art. 8 Nr. 1 DSGVO).

viduellen Abruf eines*einer Empfängers*Empfängerin erbracht werden (vgl. *Kamm 2020*). Die Zustimmung für die Datenverarbeitung im Zuge der Teilnahme an einem Zeltlager durch Minderjährige fällt somit beispielsweise nicht unter »Dienste der Informationsgesellschaft« und muss durch die Erziehungsberechtigten bestätigt werden (ebd.).

Das DSG-EKD und auch die DSGVO beziehen sich nur auf die datenschutzrechtlichen Aspekte. Ob und wie Minderjährige ggf. Verträge, auch im Kontext ihrer personenbezogenen Daten, abschließen können, ist jeweils in anderen Gesetzen geregelt (vgl. *Schrock 2018*).

3.2 Adress- und Mitgliederverwaltung

§
Art. 6 Nr. 5 DSG-EKD

Laut Art. 6 Nr. 5 des Datenschutzgesetzes der Evangelischen Kirche in Deutschland ist die Verarbeitung von personenbezogenen Daten zulässig, wenn dies »zur Erfüllung eines Vertrags […]« erforderlich ist. Dies bedeutet für die Arbeit im VCP, dass alle Daten erhoben werden dürfen, welche für das Erreichen der Verbandsziele laut Satzung sowie für die Durchführung des Mitgliedschaftsvertrags notwendig sind (vgl. *Weller 2020: 25*). Diese personenbezogenen Daten sind beispielsweise in der Mitgliederverwaltung der Name, die Anschrift, das Geburtsdatum oder auch eine Bankverbindung.

§
Art. 5 Nr. 1–2 DSG-EKD

Die Grundätze des Datenschutzes, wie in Art. 5 Nr. 1–2 des DSG-EKD festgelegt, bleiben jedoch auch hierbei bestehen (siehe Kapitel 1.2). Funktionsträger*innen dürfen daher nur solche Daten verarbeiten, die sie zur Erfüllung ihrer Aufgaben benötigen (vgl. *Weller 2020: 31*). Die Zuständigkeiten und somit die Aufgabenverteilung sind dabei der Satzung, den Ordnungen oder auch Geschäftsverteilungsplänen zu entnehmen. So ist es beispielsweise notwendig, dass das Küchenteam Allergien und Lebensmittelunverträglichkeiten der Teilnehmer*innen kennt. Die gleichen Informationen sind jedoch für die Aufgabenerfüllung von Mitarbeiter*innen im Bereich der Infrastruktur oder Öffentlichkeitsarbeit nicht relevant und sollten somit auch nicht zugänglich sein.

Wichtig zu beachten ist, dass diese Ausnahme vom Verarbeitungsverbot nur dann Geltung hat, wenn es sich um die Verarbeitung personenbezogener Daten durch dafür zuständige Funktionsträger*innen des Verbands/Vereins handelt (ebd.). Dem entgegen sind andere VCPer*innen im Verhältnis zum VCP »Dritte«, an welche Daten nicht ohne Zustimmung weitergegeben werden dürfen (ebd.). Dies ist nur dann zulässig, wenn es laut Satzung für die Durchführung bestimmter Vorgänge notwendig ist.

So ist beispielsweise für die Einberufung einer außerordentlichen Bundesversammlung satzungsgemäß eine Mindestanzahl an Antragstel-

ler*innen notwendig. Dementsprechend dürften beteiligte VCPer*innen vereinsrechtlich Einsicht in Adresslisten oder Mitgliederdaten erhalten, um weitere Unterstützer*innen für ihren Antrag zu gewinnen. Doch auch, wenn eine solche Weitergabe personenbezogener Daten an »VCP-Dritte« zum Zweck der satzungsgemäßen Aufgabenerfüllung des VCP grundsätzlich rechtlich möglich ist, ist beispielsweise die Einbindung der Bundeszentrale, welche als zuständiges Funktionsorgan ohnehin Zugriff auf die Daten hat, für Übermittlungszwecke vorzuziehen (vgl. *Kamm 2020*). So kann etwa eine E-Mail mit der Bitte um Weiterleitung durch die Bundeszentrale im bcc an den anvisierten Empfänger*innenkreis gesendet werden. Dies ist datenschutzrechtlich die gesicherte Variante und personenbezogene Daten müssen nicht durch mehr Hände als unbedingt notwendig gehen (ebd.).

Die Verarbeitung personenbezogener Daten von Mitgliedern ist rechtmäßig, wenn es für das Funktionieren des Verbands/Vereins notwendig ist und hilft, seine Verbandsziele laut Satzung zu erreichen (vgl. *Weller 2020: 36*). Auf eine zusätzliche Einwilligung kann verzichtet werden.

3.3 Anmeldedaten für VCP-Veranstaltungen

§
Art. 5 Nr. 1 DSG-EKD

Veranstaltungen, ob Versammlungen, Lager, Netzwerktreffen oder Fach- und Projektgruppentreffen, sind fester Bestandteil des Verbandslebens. Die Anmeldedaten von Teilnehmer*innen sind personenbezogene Daten und somit nach den generellen Grundsätzen des Datenschutzes zu behandeln. Dabei macht es keinen datenschutzrechtlichen Unterschied, ob Anmeldungen über ein Online-Formular oder in Papierform erfolgen. Wichtig ist in jedem Fall, dass Teilnehmer*innendaten vor dem unbefugten Zugriff Dritter geschützt sind, vertraulich behandelt werden und das Prinzip der Datenminimierung – nur so viele Daten wie absolut notwendig – beachtet wird (vgl. *Art. 5 Nr. 1 DSG-EKD*). Dafür sollten geeignete technische Sicherheitsvorkehrungen wie eine SSL-Verschlüsselung und organisatorische Maßnahmen wie der Einschränkung des Kreises, der Zugriff auf die Teilnehmer*innendaten hat, getroffen werden.

Generell gilt dabei, dass bei einer aktiven Anmeldung durch die Teilnehmer*innen selbst keine weiteren Einverständniserklärungen für die Verarbeitung personenbezogener Daten zur Durchführung, Planung und Nachbereitung dieser Veranstaltung eingeholt werden müssen (vgl. *Schrock 2018*). Dies ist durch die Anmeldung bereits abgedeckt (ebd.). So können Kontaktdaten von Teilnehmer*innen für vorbereitende Infomails verwendet und bei Veranstaltungen, die in einer externen Tagungsstätte stattfinden,

beispielsweise Lebensmittelallergien an das Küchenteam weitergegeben werden, ohne, dass hierfür eine erneute Zustimmung notwendig ist (Art. 6 Nr. 4 & 8 DSG-EKD).

§
Art. 6 Nr. 4 & 8 DSG-EKD

Personenbezogene Daten, die im Rahmen des Kinder- und Jugendplans des Bundes zur Förderung der Jugendarbeit über sogenannte »KJP-Listen« erfasst werden, dienen dem Erhalt und der Zukunftsfähigkeit des VCP. Somit besteht seitens der Veranstalter*innen und auch der Teilnehmer*innen einer Veranstaltung ein »berechtigtes Interesse« an der Datenweitergabe (vgl. *Art. 6 Nr. 1 & 8 DSG-EKD*; vgl. *Reichmann 2018: 19*). Dies bedeutet, dass die Erhebung und Verarbeitung der hierfür notwendigen personenbezogenen Daten auch keine explizite Einverständniserklärung benötigen und mit der Anmeldung zur Veranstaltung implizit ihrer Weitergabe zugestimmt wurde (ebd.). Wichtig ist hierbei jedoch, dass Zuschusslisten nicht offen für alle frei einsehbar ausgelegt, sondern in einer Mappe o. ä. aufbewahrt und nur von den verantwortlichen Personen eingesehen werden können (ebd.). Ähnlich verhält es sich bei der Weitergabe von personenbezogenen Daten für den Abschluss von Versicherungen für die Teilnehmer*innen. Auch hier haben sowohl die Teilnehmer*innen als auch die Veranstalter*innen »berechtigtes Interesse« an einer Datenweitergabe (ebd.). In beiden Fällen gilt jedoch, dass auch hier der Grundsatz der Datenminimierung einzuhalten ist (ebd.).

§
Art. 6 Nr. 1 & 8 DSG-EKD

Nach Abschluss einer Veranstaltung haben die Teilnehmer*innen das Recht auf Löschung ihrer personenbezogenen Daten (vgl. *Art. 21 Nr. 1 DSG-EKD*). Veranstalter*innen sind daher angehalten, Daten aktiv zu löschen, wenn sie nicht mehr für den eigentlichen Zweck der ursprünglichen Verarbeitung gebraucht werden. Dies sollte bestenfalls in einem automatisierten Verfahren oder nach einem Löschkonzept geschehen (vgl. *Kamm 2020*). Wichtig zu beachten sind dabei jedoch die gesetzlichen Aufbewahrungsfristen. Ein Beispiel hierfür ist etwa, dass Essenswünsche bereits kurz nach der Veranstaltung gelöscht werden können, da sie nicht mehr benötigt werden. Namen und Anschriften der Teilnehmer*innen müssen jedoch für den Fall von Regressforderungen weiterhin für die Dauer der gesetzlich geregelten Aufbewahrungsfrist gespeichert werden (vgl. *Schrock 2018*). Ähnlich verhält es sich auch mit Bankunterlagen, Kontoauszügen, Buchungs- und alle weiteren Belege, welche nach geltendem Steuerreicht zehn Jahre aufbewahrt werden müssen. Für Verträge, Versicherungspolicen, Angebote und Auftragsbestätigungen sowie Mahnungen beträgt diese Frist sechs Jahre. Deswegen muss auch nach Ende einer Veranstaltung genau differenziert werden, welche Daten rechtlich bindend aufbewahrt und welche personenbezogenen Daten im Sinne des Rechts auf Löschung vernichtet werden müssen.

§
Art. 21 Nr. 1 & 4 DSG-EKD

Anmeldeverfahren und Teilnehmer*innenmanagement sind häufige, datenschutzrechtlich wichtige Tätigkeiten, mit denen Leitungen und

hauptberufliche Mitarbeiter*innen konfrontiert werden. Die Grundsätze lauten hierbei:

- Nur solche personenbezogenen Daten werden erhoben, die unbedingt für eine Veranstaltung notwendig sind.
- Nur Personen, die diese Daten im Rahmen der Veranstaltung benötigen, haben Zugriff darauf.
- Personenbezogene Daten werden gelöscht, sobald sie nicht mehr für ihren eigentlichen Zweck relevant sind und die gesetzliche Aufbewahrungsfrist abgelaufen ist.

3.4 Datenweitergabe zwischen Verband, Vereinen und Stiftungen des VCP

§
Art. 6 Nr. 4 DSG-EKD

Der VCP wird in seiner täglichen Arbeit finanziell, materiell und organisatorisch durch seine Stiftungen und auch kleine Vereine auf Stammes- und Landesebene unterstützt. Dabei werden auch personenbezogene Daten von VCP-Mitgliedern weitergegeben und durch diese Stellen verarbeitet. Datenschutzrechtlich ist dieser Austausch grundsätzlich möglich (vgl. *Kamm 2020*). Dies ist darin begründet, dass es sich bei der Sicherstellung oder Förderung der Finanzierung einer kirchlichen Einrichtung, wie sie der VCP ist, um eine Aufgabe im kirchlichen Interesse handelt (ebd.). Vereine oder Stiftungen unterstützen so den VCP bei der Erfüllung seines satzungsmäßigen Zwecks.

Die Verarbeitung liegt dabei auch im berechtigten Interesse eines*einer Dritten, in diesem Fall der Stiftung oder des Vereins, an der Finanzierung des VCP (ebd.). Schutzwürdige Interessen der betroffenen Personen, also der beworbenen Vereins- bzw. Verbandsmitglieder, sind hingegen nicht ersichtlich. Es ist vielmehr auch in ihrem eigenen Sinn, dass die Finanzierung des Verbands und somit dessen dauerhafter Bestand gesichert sind (ebd.). Eine Finanzierung auf Spendenbasis für Verbände ist dabei nicht unüblich, so dass es sich auch nicht um eine unerwartete Datenverarbeitung für die betroffenen Personen handelt (ebd.).

VCP-Mitglieder haben jedoch jederzeit das Recht, der Datenverarbeitung durch Vereine oder Stiftungen mit Blick auf die Zukunft zu widersprechen. Diese Möglichkeit stellt den Rechtsschutz der VCP-Mitglieder sicher und muss den betroffenen Personen bekannt sein.

Personenbezogene Daten dürfen an Stiftungen bzw. Vereine des VCP weitergegeben werden, solange hierdurch die Aufgabenerfüllung des VCP gesichert und gefördert wird. VCP-Mitglieder haben jedoch mit Blick auf die Zukunft das Recht, dieser Weitergabe zu widersprechen.

3.5 Verpflichtung auf das Datenschutzgeheimnis

VCP-Mitglieder haben das Recht, dass ihre personenbezogenen Daten vertraulich und gewissenhaft behandelt werden und der Datenschutz von allen Ebenen und Mitarbeiter*innen eingehalten wird. Aus diesem Grund muss, wer als ehrenamtliche*r oder hauptberufliche*r Mitarbeiter*in des VCP regelmäßig mit personenbezogenen Daten umgeht, durch das zuständige Gremium oder Organ auf das Datengeheimnis verpflichtet werden (BfD EKD 2018b).[10] Die Grundprämisse dieser Verpflichtungserklärung ist dabei, dass bestätigt wird, dass personenbezogene Daten nicht unbefugt verarbeitet oder weitergegeben werden und das Datengeheimnis auch nach Beendigung einer Tätigkeit weiterhin Bestand hat. Dabei ist eine Verpflichtungserklärung kein Ausdruck von Misstrauen, sondern vielmehr ein Qualitätsmerkmal eines Verbands.

Generell gilt, dass immer zwei Ausführungen einer Datenschutzverpflichtung notwendig sind – eine verbleibt bei der verpflichteten Person und die andere wird an das Gremium, dem diese*r Funktionsträger*innen angehört, weitergegeben. Damit alle Mitarbeiter*innen des VCP, egal ob ehrenamtlich oder hauptberuflich, auch ausreichend informiert dieser Erklärung zustimmen können, muss zunächst eine Datenschutzschulung unter *https://datenschutz-schulung.vcp.de/*absolviert werden. Anschließend muss eine der beiden Verpflichtungserklärungen auf das Datengeheimnis an die VCP-Bundeszentrale als verantwortliche Organisationseinheit gesendet werden.

Nach Abschluss dieser Schritte bietet die VCP-Bundeszentrale den Mitarbeiter*innen der Landesbüros, Landes- und Stammesleitungen an, Einsicht auf die Mitgliederdatenbank ihrer jeweiligen Untergliederung mittels einer Websoftware (eVEWA) zu nehmen.

3.6 Schadensersatz und Strafen

Die gesetzlichen Regelungen und das kirchliche Datenschutzrecht sind in erster Linie zum Schutz von Menschen in Kraft getreten. Um diese Sicherheit zu gewährleisten, sieht das deutsche Datenschutzrecht auch Strafen bei grober Missachtung dieser Regelungen vor. Grundsätzlich gilt, dass der Vereins- bzw. Verbandsvorstand gegenüber dem Verein, und

10 Das DSG-EKD fordert ausdrücklich, dass alle Personen, die personenbezogene Daten verarbeiten, auf das Datengeheimnis verpflichtet werden. In der DSGVO ist diese explizite »Muss-Forderung« nicht mitaufgenommen. Im Rahmen des Gesamtverbands VCP wird hier das DSG-EKD als weitreichendere Regelung angewendet.

damit seinen Mitgliedern, in der Pflicht steht, die geltenden Vorschriften einzuhalten und umzusetzen (vgl. *Weller 2020: 83*). Verstößt ein Vorstand bzw. eine Leitung gegen diese Pflicht und entsteht hieraus ein Schaden für die betroffenen Personen, kann der Verein/Verband Schadensersatzansprüche gegenüber seinem Vorstand bzw. seiner Leitung geltend machen (ebd.). Dies ist jedoch nur dann gegeben, wenn ehrenamtliche Vorsitzende, wie sie der VCP hat, vorsätzlich oder grob fahrlässig handeln (§ 31 a BGB).

§
Art. 31a BGB

§
Art. 48 DSG-EKD

Im kirchlichen Datenschutzrecht heißt es hierzu u. a. in Art. 48 DSG-EKD:[11]

(1) Jede Person, der wegen einer Verletzung der Regelungen über den kirchlichen Datenschutz ein Schaden entstanden ist, hat nach diesem Kirchengesetz Anspruch auf Schadensersatz gegen die verantwortliche Stelle. Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(2) Eine verantwortliche Stelle wird von der Haftung gemäß Absatz 1 befreit, wenn sie nachweist, dass sie für den eingetretenen Schaden nicht verantwortlich ist.

Es ist sicherzustellen, dass Mitarbeiter*innen, ehrenamtlich oder hauptberuflich, über ihre Pflichten und Verantwortlichkeiten gegenüber dem Datenschutz Bescheid wissen (vgl. *Weller 2020: 84*). Es ist dabei die Aufgabe des Vorstands bzw. der Leitung, die Personen, welche personenbezogene Daten verarbeiten, aufzuklären und zum Einhalten der Regelungen aufzufordern (ebd.). Diese Aufgabe kann jedoch auch an die*den örtlich Beauftragte*n für den Datenschutz delegiert werden. Wenn dennoch Personen eingesetzt werden, die das notwendige Wissen über den Datenschutz nicht haben, kann, wie oben dargestellt, dem Vorstand bzw. der Leitung als einsetzender Stelle bei Auftreten eines Datenschutzverstoßes möglicherweise Fahrlässigkeit unterstellt werden. In diesem Fall kann der Verein/Verband bei ihm*ihr etwaige resultierende Schadensansprüche geltend machen (vgl. *Weller 2020: 83*).

---

11 Analog Art. 82 DSGVO:

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. […]

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Wenn ein Verein oder Verband seinen Pflichten nach dem DSG-EKD nicht nachkommt, drohen Geldbußen, Geldstrafen oder gar Freiheitsstrafen. In den meisten Fällen sind Strafen für gemeinnützige Vereine, insbesondere bei Erstverstößen, im Vergleich zu kommerziellen Unternehmen eher gering (*vgl. Weller 2020: 83*). Bei groben und schwerwiegenden Verstößen können sie dennoch empfindlich ausfallen.

Sichere Kommunikation

4

Die Kommunikation im Privat-, aber auch Verbandsleben verlagert sich immer mehr in den digitalen Raum. Ob Messenger, E-Mail oder andere Onlinedienste, diese bequeme Art des Austauschs verdrängt das klassische Telefonat oder den Brief zusehends. Dabei werden auch immer wieder personenbezogene Daten übermittelt – seien es die eigenen oder die anderer VCP-Mitglieder. Das geltende Datenschutzrecht verlangt daher, dass auch diese Kommunikationswege unter Risikoaspekten bewertet und »geeignete technische und organisatorische Maßnahmen« getroffen werden (vgl. *Art. 27 Nr. 1 DSG-EKD*). In diesem Kapitel wird deshalb der Umgang mit personenbezogenen Daten von Amtsträger*innen bzw. Funktionsträger*innen erklärt sowie die gängigsten Kommunikationsmittel im Hinblick auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht dargestellt.

§
Art. 27 Nr. 1 DSG-EKD

4.1 Kommunikationsdaten von Amts- und Funktionsträger*innen

Generell sind die persönlichen Daten von Mitgliedern eines Verbands vertraulich zu behandeln und nicht öffentlich zu machen. Doch gibt es, wie bereits weiter oben beschrieben, auch Ausnahmen von dieser Regelung (vgl. *Art. 6 Nr. 1 DSG-EKD*). Ein Beispiel hierfür sind die Namen und Kontaktdaten von Vorsitzenden, der*des örtlich Beauftragten für den Datenschutz oder auch der Pressestelle. Dies ist begründet in der Annahme, dass Vereine oder Verbände ihren Zweck ohne die Veröffentlichung von Ansprechpartner*innen nicht erfüllen können, wodurch ein berechtigtes Interesse des Vereins vorliegt (vgl. *Weller 2020: 44*). Jedoch können zur Wahrung der Privatsphäre spezielle Kommunikationsdaten durch den Verband eingerichtet werden (ebd.).

§
Art. 6 Nr. 1 DSG-EKD

So kann beispielsweise für Vorstände *(vorstand@musterverband.de)* und auch für die Pressestelle *(presse@musterverband.de)* eine generische E-Mail-Adresse als Anlaufstation geschaffen werden. So müssen Privatadressen nicht preisgegeben werden und die Privatsphäre bleibt geschützt. Die Erreichbarkeit wichtiger Ansprechpartner*innen des Verbands/Vereins ist aber dennoch gewährleistet.

4.2 Sicherheit in der E-Mail-Kommunikation

E-Mails werden zwar zunehmend von anderen Kommunikationsmitteln abgelöst, sind jedoch trotzdem aus dem heutigen Leben nicht wegzudenken. Sie werden zur Kommunikation in verschiedensten Situationen, wie zum Beispiel für Einladungen zu Veranstaltungen, verwendet und

sind so ein Kommunikationsmittel, das, insbesondere wenn Revisionssicherheit notwendig ist, weiterhin benutzt wird. Da E-Mails jedoch oftmals auch personenbezogene Daten enthalten, ist es wichtig, dass der E-Mail-Verkehr in jedem Fall über eine sichere Verbindung erfolgt. Dabei muss die Verschlüsselung die Verbindung zum E-Mail-Dienst und zum E-Mailserver, die E-Mail selbst sowie archivierte E-Mails umfassen (vgl. *Kamm 2020*).

Um eine sichere Verbindung zum E-Mail-Dienst (beispielsweise *gmx.de* oder *web.de*) über eine Weboberfläche aufzubauen, muss eine Secure Socket Layer- (SSL-) und eine Transport Layer Security- (TLS-) Verschlüsselung bestehen. Diese ist daran erkennbar, dass die Webseiten-URL mit »https« anstelle des üblichen »http« beginnt. Bei den meisten E-Mail-Angeboten ist dies bereits automatisch der Fall und gehört mittlerweile zum Standard. Die E-Mail selbst wird jedoch nicht automatisch verschlüsselt verschickt. Dies muss in der jeweiligen Weboberfläche des E-Mail-Accounts oder im Client-Programm (zum Beispiel Microsoft Outlook) speziell eingestellt werden. Nur so können E-Mails sicher und datenschutzkonform versendet und empfangen werden.

4.3 Messenger und Online-Dienste

Messenger-Dienste sind ein beliebtes Kommunikationsmittel. Statistiken zeigen, dass beispielsweise WhatsApp von 96 % der 16- bis 24-Jährigen täglich oder mehrmals in der Woche verwendet wird (vgl. *Bundesnetzagentur 2020*). In Bezug auf das geltende Datenschutzrecht sind jedoch bei deren Benutzung einige Aspekte kritisch zu betrachten. Dabei gilt: Obwohl verschiedene Messenger-Dienste personenbezogene Daten in unterschiedlicher Weise verarbeiten, muss das allgemeine Sende- und Empfangsrisiko immer auf Grundlage fester Kriterien bewertet werden (vgl. *BfD EKD 2018a: 2*):

- Die Ende-zu-Ende-Verschlüsselung der über den Messenger-Dienst ausgetauschten personenbezogenen Daten muss gewährleistet sein.
- Die Nutzung der empfangenen personenbezogenen Daten durch den E-Mail-Dienst darf ausschließlich zum Zweck der Übertragung der Nachrichteninhalte zwischen den Teilnehmer*innen einer Unterhaltung dienen.
- Die unberechtigte Weitergabe von Kontaktdaten an den Messenger-Dienst, insbesondere durch Übermittlung des auf dem eingesetzten Endgerät gespeicherten Telefonbuchs, muss ausgeschlossen sein.
- Besondere zusätzliche datenschutzrechtliche Anforderungen gelten für Messenger-Dienste, die Nutzer*innendaten auch in Drittländern (Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums) verarbeiten.

Auf Grundlage dieser Kriterien hat die Evangelische Kirche in Deutschland Tipps mit datenschutzrechtlichen Hinweisen zur Nutzung von Messenger-Diensten veröffentlicht:[12]

- ***WhatsApp:*** Obwohl dieser Dienst eine Ende-zu-Ende-Verschlüsselung anbietet, bleibt die zugrunde liegende Systematik intransparent (vgl. *Kamm 2020*). Es werden Daten über Nutzungsverhalten, Kontakte und andere Informationen an Facebook übermittelt, ohne dass dies für den*die Nutzer*in nachvollziehbar ist. Ein weiterer datenschutzrechtlich bedenklicher Aspekt stellt die Übermittlung von Daten an ein sog. Drittland, in diesem Fall die USA, dar, was unter geltendem Recht problematisch ist. In den AGB wird außerdem darauf hingewiesen, dass WhatsApp lediglich für den privaten Gebrauch genutzt werden darf. Eine Nutzung im VCP-Kontext kann somit gegen die Nutzungsbestimmungen des Unternehmens verstoßen (ebd.). Auf Grundlage dieser datenschutzrechtlichen Bedenken wird eine Verwendung im dienstlichen Bereich nicht empfohlen.

- ***Telegram:*** Auch bei diesem Messenger-Dienst gibt es erhebliche Datenschutzbedenken, ähnlich denen bei der Verwendung von WhatsApp, weshalb von der dienstlichen Nutzung dieses Dienstes abgeraten wird (vgl. *BfD EKD 2018a: 2*).

- ***Signal:*** Bei Signal findet die Verarbeitung personenbezogener Daten außerhalb des Geltungsbereichs der DSGVO bzw. des DSG-EKD statt und stellt somit ein datenschutzrechtliches Problem dar (ebd.). Seitens der Evangelischen Kirche wird von der Nutzung dieses Dienstes im Rahmen einer beruflichen oder ehrenamtlichen Tätigkeit abgeraten.

Es gibt jedoch auch Messenger-Dienste, die bei korrektem Nutzer*innenverhalten unter Datenschutzgesichtspunkten unbedenklich sind:

- ***SIMSme (Business)*** und ***Threema (Work)***: Gegen den Einsatz dieser Messenger-Dienste, welche auf Servern in Deutschland bzw. der Schweiz gehostet werden, bestehen zurzeit keine Datenschutzbedenken seitens des*der Beauftragten für den Datenschutz der Evangelischen Kirche (ebd.). Es muss hierbei jedoch im VCP-Kontext immer sichergestellt werden, dass die Verwendung des Messenger-Dienstes in den Nutzungsbedingungen auch für den dienstlichen Einsatz gestattet ist (ebd.). Dies ist bei SIMSme Business und Threema Work auf jeden Fall gegeben. Diese speziellen Varianten setzen zudem noch stärker auf Verschlüsselung und Transparenz (vgl. *Kamm 2020*).

12 Die Hinweise und Empfehlungen der EKD haben auch für VCP-Länder, die unter die DSGVO fallen, Gültigkeit.

- ***Wire*** und ***Wire Pro***: Der Einsatz dieses Messenger-Dienstes ist datenschutzrechtlich unbedenklich. Mit Sitz innerhalb des Geltungsbereiches des DSG-EKD bzw. der DSGVO und einer Ende-zu-Ende-Verschlüsselung der Kommunikation werden die herrschenden Richtlinien eingehalten (vgl. *Kamm 2020*).

- ***Rocket Chat***: Dieser Messenger-Dienst kann, solange auf einem eigenen Server oder auf einer europäischen Cloud gehostet, in Bezug auf das geltende Datenschutzrecht genutzt werden. Auch hier ist die Ende-zu-Ende-Kommunikation sichergestellt (vgl. *Kamm 2020*).

- ***Eigene Messenger-Dienste***: Die Entwicklung sowie der Einsatz und Betrieb eines eigenen Messenger-Dienstes auf Basis von etablierten und frei zugänglichen Protokollen auf Servern in Deutschland bzw. im Geltungsbereich der DSGVO bzw. des DSG-EKD ist aus Sicht des*der Beauftragten für den Datenschutz der EKD die beste Lösung und wird daher klar empfohlen (vgl. *BfD EKD 2018a: 2*).

Festzuhalten ist dabei, dass der Einsatz von WhatsApp und Messengern mit vergleichbaren Parametern durch Funktionsträger*innen des VCP (ehrenamtlich und hauptberuflich) zur Erfüllung kirchlicher Zwecke, und damit im Rahmen der VCP-Arbeit, datenschutzrechtlich erheblich risikobehaftet ist (vgl. *Kamm 2020*). Im Falle datenschutz- oder zivilrechtlicher Verstöße durch Funktionsträger*innen sind die Verantwortlichen des VCP bzw. der jeweiligen Untergliederungen haftbar, wenn sie den Einsatz dieser Messenger und ähnlicher Apps angeordnet oder ausdrücklich gebilligt haben (ebd.).

Grundsätzlich müssen sich der VCP und seine Untergliederungen daher an folgende Spielregeln halten (vgl. *Kamm 2020*):

- Keine Verwendung nicht genehmigter Messenger auf dienstlichen Endgeräten
- Keine Erfüllung kirchlicher Zwecke unter Verwendung nicht genehmigter Messenger
- Keine Speicherung von Kontaktdaten aus dem dienstlichen Gebrauch auf einem Privatgerät, auf dem nicht genehmigte Messenger verwendet werden

> Das kirchliche beziehungsweise öffentliche Datenschutzrecht regelt nicht nur die Verwendung von Messenger-Diensten durch hauptberufliche Mitarbeiter*innen des VCP. Es gilt für alle haupt- oder ehrenamtlichen Funktionsträger*innen – bis in die Stämme und Gruppen.

Die hier dargestellten Tipps und Hinweise zu Messenger-Diensten stellen eine Momentaufnahme dar und Änderungen in den Nutzungsbe-

dingungen und Serverstandorten sind jederzeit möglich. Die Nutzung mobiler Endgeräte und Messenger-Dienste birgt generell ein hohes Datenschutzrisiko, so dass eine Risikoanalyse zur konkreten Situation im Einzelfall generell immer zu empfehlen ist (ebd.). Auf das Attribut »datenschutzkonform« bei Messenger-Diensten sollte sich dabei nicht ausschließlich verlassen werden. Dies kann irreführend sein und stellt keine Garantie dafür dar, dass personenbezogene Daten auch sicher sind. Denn Datenschutzkonformität ist nur dann sichergestellt, wenn sich alle drei beteiligten Komponenten an die Vorgaben des DSG-EKD bzw. der DSGVO halten: Absender*in, Messenger-Dienst und Empfänger*in.

4.4 Webkonferenzen

Webkonferenzen werden gerade in der heutigen Zeit immer beliebter, um Absprachen zu treffen und online Veranstaltungen durchzuführen. Unterschiedliche Dienste bieten eine Vielzahl an Möglichkeiten an. Bei der Auswahl einer geeigneten Software für Webkonferenzen sind unter datenschutzrechtlichen Aspekten folgende Optionen in der dargestellten Reihenfolge zu bevorzugen:

- Selbst entwickelte Software oder Open Source Software auf eigenen Servern oder durch Serverdienstleistungen im Geltungsbereich des DSG-EKD bzw. der DSGVO
- Deutsche bzw. europäische Dienste (inkl. der Schweiz) auf eigenen Servern oder Angebote von Serverdienstleistungen im Geltungsbereich des DSG-EKD bzw. der DSGVO
- Deutsche oder europäische Dienste (inkl. Schweiz), die zum Betrieb der Software Serverdienstleistungen aus Drittländern einsetzen
- Dienste aus Drittländern

Angebote der VCP-Bundesebene, welche diese Vorgaben zum Datenschutz erfüllen, sind aktuell:

- ***Jitsi***: Der Betrieb von Jitsi erfolgt auf gehosteten Servern in Deutschland und es wurde ein Auftragsverarbeitungsvertrag mit den Verantwortlichen der Plattform geschlossen. VCP-Meet (*https://meet.vcp.de*) ist dabei eine Plattform, welche von allen VCP-Ebenen genutzt werden kann. Sie bietet eine schnelle und einfache Lösung für digitale Gruppenstunden, Stammesrunden und viele weitere Formate.

- ***Zoom:*** Der hierfür verwendete Server befindet sich in Deutschland und untersteht somit dem geltenden Datenschutzrecht. Zusätzliche Sicherheit bieten ein abgeschlossener Auftragsverarbeitungsvertrag sowie eine Zusatzvereinbarung zwischen dem Zoom-Unternehmen Connect4Video (easymeet24) und dem VCP.

- ***Microsoft365 (u. a. Microsoft Teams)***: Zur datenschutzkonformen Nutzung der Microsoft-Dienste (Microsoft365) wurde ein Auftragsverarbeitungsvertrag inkl. Zusatzvereinbarung mit Microsoft abgeschlossen. Hiermit unterwirft sich Microsoft den aktuell geltenden Bestimmungen des Datenschutzgesetzes der Evangelischen Kirche (DSG-EKD) und der Datenschutzaufsicht der Evangelischen Kirche in Deutschland. Zudem werden die (Cloud-)Daten auf Servern in Deutschland gespeichert.

Grundsätzlich gilt, dass der Betrieb auf eigenen Servern bzw. Servern im Geltungsbereich des DSG-EKD/der DSGVO für Webkonferenzen anzustreben ist, um datenschutzrechtlich auf der sicheren Seite zu stehen.

Der Verband in der Öffentlichkeit

5

Als Kinder- und Jugendverband möchten wir zielgruppengerecht informieren. Während gerade in Stämmen und Gruppen vor Ort hierfür auch das »Schwarze Brett« oder die traditionelle Infopost noch zum Tragen kommen, wird insbesondere ab der Regionsebene auf die Informationsweitergabe über internetbasierte Medien gesetzt. Doch egal, ob es sich um eine eigene Webseite, Facebookseite oder auch ein öffentliches Messagingboard handelt, müssen auch hier die Nutzer*innen darüber informiert werden, ob und wie ihre personenbezogenen Daten (zum Beispiel ihre IP-Adresse) erhoben, verarbeitet und gespeichert werden (vgl. *Weller 2020: 123*).

Generell ist bei der Veröffentlichung von personenbezogenen Daten im Internet zu beachten, dass einmal veröffentlichte Daten nur sehr schwer oder gar nicht wieder gelöscht werden können. Auch kann nicht gewährleistet werden, dass diese Daten nicht verfälscht werden und somit ein ganz anderes Licht auf die betroffene Person werfen als das Bild, welches ursprünglich dargestellt werden sollte (vgl. *Weller 2020: 36*). Das »World Wide Web« ist, wie der Name schon sagt, weltweit verfügbar, so dass Daten auch in Staaten, in denen nicht das DSG-EKD oder die DSGVO Anwendung finden, verarbeitet und gespeichert werden können (ebd.). Diese Tatsachen begründen den Grundsatz zur Veröffentlichung von personenbezogenen Daten im Internet: Genau prüfen, Einverständnis einholen und so wenig wie möglich preisgeben.

5.1 Die Datenschutzerklärung

§
Art. 16–19 DSG-EKD

Eine Datenschutzerklärung gehört mittlerweile nach geltendem Recht zu jedem Internetauftritt. Das Telemediengesetz (TMG) ist dabei aktuell noch die bestimmende Rechtsgrundlage für Internetauftritte. Doch insbesondere in Bezug auf die Informationspflichten wird es zunehmend vom DSG-EKD und der DSGVO überlagert (vgl. *Weller 2020: 123*). Für VCP-Internetauftritte bedeutet dies daher, dass die Datenschutzerklärung auf einer Vereins- oder Gliederungswebseite auf den Artikeln 16 bis 19 der DSG-EKD[13] beruhen müssen (ebd.). Die Informationspflichten sind dabei relativ umfangreich, da betroffene Personen über alle Datenverarbeitungsprozesse und die Rechtsgrundlagen für diese Verarbeitung informiert werden müssen (vgl. *Schrock 2018*).

Für die Erstellung einer so umfassenden Datenschutzerklärung kann dabei beispielsweise ein Datenschutz-Generator, der im Internet kostenlos abgerufen werden kann, zu Hilfe genommen werden (ebd.). Wichtig zu beachten ist hierbei jedoch, dass auch bei Nutzung eines solchen Generators Grundkenntnisse der technischen Voraussetzungen der Webseite (wie und wo werden welche Daten gespeichert) und auch Kenntnis des

13 Analog hierzu Art. 12–15 DSGVO.

gültigen Datenschutzrechtes vorhanden sein müssen, um gegebenenfalls notwendige Spezifikationen zur Anpassung an Vereins- oder Verbandsbedürfnisse vorzunehmen (ebd.). Alternativ zu diesen allgemeinen Generatoren kann auch die Arbeitshilfe der EKD für die eigenständige Erstellung einer Datenschutzerklärung verwendet werden. Diese kann unter *https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-erstellung-einer-datenschutzerklaerung/* abgerufen werden.

Auch bei digitalen Veranstaltungen müssen Teilnehmer*innen über dabei evtl. erhobene und verarbeitete personenbezogene Daten (zum Beispiel Aufzeichnung der Sitzung für das Protokoll, Veröffentlichung der Teilnehmer*innenliste) durch eine Datenschutzerklärung aufgeklärt werden (vgl. *Weller 2020: 123*). Diese Erklärung kann dabei auf der Datenschutzerklärung des Dienstes der verwendeten Softwarelösung aufbauen (ebd.).

5.2 Öffentliche Film- und Fotoaufnahmen[14]

§
Art. 22 & 23 KunstUrhG

Für Foto- und Filmaufnahmen gibt es bereits seit vielen Jahren eine eigene Rechtsgrundlage – Art. 22 und Art. 23 des Kunsturhebergesetzes (Recht am eigenen Bild). Neben dieser Regelung trat im Jahr 2018 auch das DSG-EKD bzw. die DSGVO in Kraft. Fotos und Filme gelten als personenbezogene Daten, sobald eine Person identifizierbar ist. Zudem enthalten die meisten Bilder und Videos heutzutage sogenannte EXIF-Dateien, die oft auch GPS-Daten und das Datum bzw. die Uhrzeit der Aufnahme speichern. Dadurch kann zusätzlich darauf geschlossen werden, wo sich die auf dem Foto abgebildete Person und auch der*die Fotograf*in wann befunden haben. Daher benötigen Foto- und Filmaufnahmen im Sinne des Art. 6 Nr. 2 DSG-EKD die schriftliche Einwilligung der betroffenen Person vor ihrer Veröffentlichung. Eine solche Zustimmung muss für jede Veranstaltung bzw. jedes Treffen neu erteilt werden, denn von einer einmaligen Einwilligung kann nicht pauschal darauf geschlossen werden, dass sie auch für weitere Situationen gilt. Diese Vorgabe ist mit dem Grundsatz der Zweckbindung begründet (vgl. *Art. 5 Nr. 1 DSG-EKD*). Eine Vorlage für Foto- und Filmaufnahmevereinbarungen im Kontext des VCP kann unter *www.vcp.de/service/dokumente/*abgerufen werden.

§
Art. 6 Nr. 2 DSG-EKD

§
Art. 5 Nr. 1 DSG-EKD

Doch gibt es auch bei dieser Regelung Ausnahmen. In den folgenden drei Fällen können Foto- und Filmaufnahmen ohne eine schriftliche Einwilligung erstellt und veröffentlicht werden:

14 Eine ausführliche Handreichung zum Thema Foto- und Bildrechte befindet sich aktuell in Arbeit.

- ***Bei Personen der Zeitgeschichte, Stars, Politiker*innen oder Prominenten:***
  Wenn beispielsweise das Friedenslicht an eine*n Minister*in überreicht wird, bedarf es für die Veröffentlichung eines Bildes dieser Übergabe zwar eine Einverständniserklärung der auf dem Foto abgebildeten VCPer*innen, jedoch nicht der Ministerin*des Ministers als Person des öffentlichen Lebens. Ein anderes Beispiel wäre der Spatenstich für ein neues Stammesheim durch eine bekannte Persönlichkeit. Auch diese sind von einer expliziten Einverständniserklärung ausgeschlossen.

- ***Bei einer Person, die als Beiwerk nur eine untergeordnete Rolle neben einer Landschaft oder Örtlichkeit spielt:***
  Dies ist beispielsweise der Fall, wenn ein Foto eines Lagerplatzes zur Werbung für das anstehende Landes- oder Stammeslager gemacht wird und dabei ein*e Spaziergänger*in am Horizont zu erkennen ist. Ein weiteres Szenario ist ein Ausflug mit Gruppenkindern zu einem bekannten Denkmal, von welchem ein Foto für einen Blogbeitrag aufgenommen wird. Es wird im Regelfall kaum gelingen, ein solches Monument zu fotografieren, ohne dass sich Menschen im Hintergrund aufhalten.

- ***Bei einer öffentlichen Veranstaltung, bei welcher eine große Menschenmenge fotografiert wird:***
  Diese Ausnahmeregelung ist für die Arbeit im VCP wahrscheinlich am wichtigsten. Es ist grundsätzlich erlaubt, im Zuge öffentlicher Veranstaltungen Bilder der Teilnehmer*innen (nicht jedoch einzeln herausgestellter Personen) in der Verbandszeitung, auf der eigenen Webseite oder auch in den sozialen Medien zu veröffentlichen. Hierfür ist das spezifische Einverständnis der betroffenen Personen nicht zwingend notwendig (vgl. *Weller 2020: 36*). In diesem Zusammenhang ist jedoch das Wort »öffentlich« entscheidend – die Veranstaltung muss für jede*n offen sein – auch für Personen, die nicht Mitglied des VCP oder dem Verband in anderer Weise verbunden sind (ebd.).
  Damit Teilnehmer*innen die Möglichkeit bekommen, sich aufgrund möglicher Foto- oder Filmaufnahmen auch gegen eine Teilnahme oder für einen »Platz im Hintergrund« zu entscheiden, muss der*die Veranstalter*in seinen*ihren Informationspflichten nachkommen. So ist auf Grundlage des Art. 17 des DSG-EKD ein sichtbarer Datenschutzhinweis anzubringen, der gesondert darauf aufmerksam macht, dass Fotos gemacht und veröffentlicht werden, auf denen ggf. Personen auch erkennbar sind (vgl. *Kamm 2020*). Zudem sollte in diesem Zuge auch ein*e Ansprechpartner*in für Fragen und Auskünfte benannt werden. Bei Veranstaltungen des VCP kommen zudem regelmäßig Informationen hinzu, die Rückschluss auf die religiöse Überzeugung liefern (könnten) und damit besondere Kategorien personenbezogener Daten offenlegen (ebd.). Dies ist dann der Fall, wenn beispielsweise

§
Art. 17 DSG-EKD

Kluften/Trachten des evangelischen Pfadfinder*innenverbands getragen werden. Hierauf muss in den o. g. Datenschutzhinweisen gesondert verwiesen werden (ebd.).
Generell sollte die Verarbeitung – wenn schon nicht in allen Fällen nach schriftlicher Einwilligung – zumindest mit soweit vertretbarem Aufwand wie möglich von der Entscheidung der betroffenen Personen abhängig gemacht werden (ebd.). Eine Lösung hierfür wäre beispielsweise ein neutraler kleiner Punkt am Kragen oder andersfarbige Namensschilder den Teilnehmer*innen anzubieten, die nicht fotografiert werden möchten (ebd.). So kann mit geringem Aufwand auch erkannt werden, wer nicht auf Film- und Fotoaufnahmen erscheinen möchte.
Zu beachten ist immer: Wenn das begründete Interesse der betroffenen Person gegenüber dem Interesse des Verbands überwiegt oder die Person einen Schaden durch die Veröffentlichung zu erwarten hat, muss auf eine Veröffentlichung verzichtet werden. Sinnvoll ist somit, die schriftliche Einwilligung zur Veröffentlichung von Film- und Fotoaufnahmen der betroffenen Personen auch bei öffentlichen Veranstaltungen einzuholen, wenn dies mit vertretbarem Aufwand möglich ist.

Minderjährige fallen unter einen besonderen Schutz bei der Veröffentlichung von Film- und Fotoaufnahmen. Während es rechtlich einige »Grauzonen« gibt, bei denen eine Veröffentlichung von Aufnahmen auch ohne explizite Zustimmung möglich ist, sollte die (schriftliche) Einwilligung durch die*den Minderjährige*n und der*des Erziehungsberechtigten die bevorzugte Variante sein.

Abschluss

6

Wichtig beim Datenschutz ist immer, im Hinterkopf zu behalten, dass hierbei zuallererst der Schutz von Menschen im Mittelpunkt steht. Dementsprechend muss mit personenbezogenen Daten vorsichtig und umsichtig umgegangen werden. Diese Handreichung soll dabei einen ersten Eindruck der wichtigsten Grundsätze der Europäischen Datenschutzgrundverordnung (DSGVO) bzw. des Datenschutzgesetztes der Evangelischen Kirche (DSG-EKD) vermitteln. Sie kann als Einstieg und Wegweiser in der Welt des Datenschutzes dienen.

Die Inhalte dieser Handreichung wurden daher mit Sorgfalt recherchiert und zusammengestellt. Dennoch können sich Richtlinien ändern und Unklarheiten auch bei größter Vorsicht einschleichen. Obwohl alle Informationen nach bestem Wissen zusammengetragen wurden, können sie keine Fachberatung im Einzelfall ersetzen. Die Verantwortlichen für den Datenschutz sind daher angehalten, auch immer eigene Recherchen für spezifische Situationen anzustellen. Bei der Suche nach weiteren Informationen und Anmerkungen zum Datenschutz im VCP steht der*die örtlich Beauftragte für den Datenschutz der VCP-Bundesebene unter *datenschutz@vcp.de* für Fragen zur Verfügung.

Anhang

7

Kleines Wörterbuch zum Datenschutz in der Verbandsarbeit

A

Aufbewahrungsfrist

Bestimmte Vertragsunterlagen und Rechnungen müssen laut Steuer- und Handelsgesetz einige Jahre aufbewahrt werden. Dies soll gewährleisten, dass auch zu einem späteren Zeitpunkt Vorgänge geprüft werden können. Die gesetzlichen Aufbewahrungsfristen liegen meist zwischen zwei und zehn Jahren.

Auftragsverarbeitung

Ein*e Auftragsverarbeiter*in verarbeitet personenbezogene Daten im Auftrag einer verantwortlichen Stelle auf Grundlage eines geschlossenen Vertrags. Die Auftragsverarbeitung kann dabei durch eine natürliche Person, aber auch eine juristische Person, einen Verein oder eine Behörde durchgeführt werden (vgl. *Verbraucherzentrale 2021*).

B

*(örtlich) Beauftragte*r für den Datenschutz*

Zur Überwachung der Einhaltung des Datenschutzes wird eine Person zum*zur örtlich Beauftragten für den Datenschutz ernannt. Dabei fällt nicht nur die Kontrolle bereits existierender Abläufe unter seine*ihre Zuständigkeit, sondern auch die Konzeptentwicklung zur besseren Einhaltung geltender Vorschriften (vgl. *Verbraucherzentrale 2021*).

Berechtigtes Interesse

»Berechtigt" im Sinne des Datenschutzes ist jedes Interesse, das aufgrund der jeweils vorliegenden Rechtsordnung gebilligt ist. Ein berechtigtes Interesse eines Verbands/Vereins an der Verarbeitung personenbezogener Daten besteht, wenn sie zum Verbandsziel und dessen Aufgabe laut Satzung beiträgt. Dabei sind vom Verein/Verband jedoch immer auch die Rechte der betroffenen Personen in die Abwägung einzubeziehen (Interessensabwägung). Wenn diese Rechte stärker wiegen als die des Vereins, dürfen die personenbezogenen Daten nicht verarbeitet werden (vgl. *Verbraucherzentrale 2021*).

Besondere Kategorien personenbezogener Daten

Bestimmte Daten sind noch sensibler als andere und deshalb besonders geschützt, da sie zum Beispiel bei Missbrauch der betroffenen Person schaden können. Diese besonderen Kategorien personenbezogener Daten dürfen datenschutzrechtlich nur unter sehr genau definierten Umständen verarbeitet werden.

D

Datenminimierung
Es dürfen nur solche personenbezogenen Daten erhoben werden, die auch tatsächlich für die vorher festgelegten, eindeutigen und legitimen Zwecke gebraucht werden. Der Grundsatz heißt hierbei: »So wenig wie nötig«.

Datenschutzerklärung
Die Datenschutzerklärung ist eine Darstellung dessen, wie ein Verein/Verband mit personenbezogenen Daten umgeht und auch, welche Daten erhoben und gespeichert werden. Sie enthält zudem Informationen zu den Schutzmaßnahmen des Vereins/Verbands und weist auf die Rechte von betroffenen Personen hin (vgl. *Verbraucherzentrale 2021*).

Datenspeicherung
Das Speichern von Daten umfasst das Erfassen und Aufbewahren von Daten auf einem Datenträger für den späteren Gebrauch.

Datenverarbeitung
Der Begriff »Datenverarbeitung« umfasst die gesamte Bandbreite dessen, was mit Daten gemacht werden kann: Erhebung, Erfassung, Speicherung, Verbreitung, Verknüpfung, Einschränkung, Löschung und Vernichtung – also letztendlich jede Form der Verwendung und Nutzung personenbezogener Daten.

Dritte*r
Eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, die nicht die betroffene Person selbst, die verantwortliche Stelle, der*die Auftragsverarbeiter*in oder eine Person ist, die unter der unmittelbaren Verantwortung der kirchlichen Stelle oder des*der Auftragsverarbeiters*Auftragsverarbeiterin befugt ist, personenbezogene Daten zu verarbeiten (vgl. *Verbraucherzentrale 2021*).

Drittland
In Bezug auf das europäische Datenschutzrecht werden alle Länder, die nicht Teil der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) sind und somit nicht unter das geltende Datenschutzrecht fallen, als Drittländer bezeichnet. Für die Übermittlung personenbezogener Daten in Drittländer gelten besondere Bestimmungen.

DSG-EKD
Das DSG-EKD ist das »Datenschutzgesetz der Evangelischen Kirche in Deutschland«. Alle Kirchengemeinden, Dekanate sowie kirchliche Einrichtungen des Öffentlichen Rechts, aber auch rechtlich selbstständige Einrichtungen und Organisationen des Bürgerlichen Rechts, die der Evangelischen Kirche organisatorisch zugeordnet sind, fallen unter dieses Datenschutzgesetz. Es ist an die einheitlichen europäischen Daten-

schutzstandards – der DSGVO – angepasst, gleichzeitig werden jedoch Besonderheiten für den kirchlichen Datenschutz berücksichtigt (vgl. *EKHN 2021*).

E

Einschränkung der Datenverarbeitung

Neben dem Recht auf Löschung gibt es im DSG-EKD auch die Möglichkeit der Einschränkung der Datenverarbeitung, wenn ein Löschen nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Diese Ausnahme ist jedoch so nicht in der DSGVO verankert.

Einwilligung/Einverständnis

Eine Einwilligung in die Datenverarbeitung ist das Einverständnis einer betroffenen Person, dass ein Verein/Verband personenbezogene Daten erheben und speichern darf. Sie muss dabei freiwillig und informiert abgegeben werden.

Erhebung

Die Erhebung von personenbezogenen Daten beschreibt das aktive und absichtsvolle Erfassen von Daten durch einen Verband/Verein.

Erlaubnisvorbehalt

Das Verbot mit Erlaubnisvorbehalt besagt, dass die Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten grundsätzlich verboten ist. Es existieren aber auch Ausnahmen des Erlaubnisvorbehalts von dieser Regelung, welche jedoch genau definiert, eng begrenzt und rechtlich geregelt sind.

F

*Funktionsträger*innen*

Ein*e Funktionsträger*innen ist im VCP ein*e ehren- oder hauptamtliche*r oder auch hauptberufliche*r Amts- oder Mandatsträger*in. Dies können Beauftrage für besondere Aufgaben (etwa Sprecher*in einer FG/PG), Leitungen auf unterschiedlichen Ebenen (beispielsweise Stammes- oder Landesleitungen) oder hauptberufliche Menschen sein, die qua Amt ein Mandat innerhalb des Verbands innehaben.

I

Informationspflicht(en)

Der Verein/Verband oder auch eine Untergliederung muss Menschen, deren personenbezogene Daten verarbeitet werden, darüber informieren, warum diese Daten erhoben und wofür sie benötigt werden, was genau mit diesen Daten gemacht wird und auch, welche Rechte sie in Bezug auf die Verarbeitung ihrer personenbezogenen Daten haben.

K

Kopplungsverbot

Personenbezogene Daten dürfen nur auf Grundlage eines freiwilligen und informierten Einverständnisses der betroffenen Person erhoben und verarbeitet werden. Das Kopplungsverbot besagt dabei, dass es nicht zulässig ist, diese Zustimmung an eine Bedingung zu knüpfen oder die Wahlmöglichkeiten so einzuschränken, dass die Freiwilligkeit nicht mehr gegeben ist.

M

Messenger-Dienste

Messenger-Dienste sind Kommunikationsmittel, bei denen durch eine sofortige Nachrichtenübermittlung zwei oder mehr Teilnehmer*innen Nachrichten meist über das Internet oder einen speziellen Server übermitteln können. Insbesondere im Bereich des Datenschutzes ist bei der Übermittlung personenbezogener Daten über Messenger-Dienste Vorsicht geboten.

Minderjährige

Minderjährige sind rechtlich alle Menschen unter 18 Jahren. Im Datenschutzrecht wird ihnen ein besonderer Schutz zuteil, da sie »besonderen Gefahren« ausgesetzt sind und sich ihrer Rechte und Risiken weniger bewusst sind.

N

Natürliche Person

Eine natürliche Person ist ein Mensch aus Fleisch und Blut als Träger*in von Rechten und Pflichten. Der Gegensatz hierzu sind »juristische Personen«, Behörden, Vereine oder Gesellschaften, deren Daten im geltenden Datenschutzrecht jedoch keine personenbezogenen Daten darstellen.

P

Personenbezogene Daten

Personenbezogene Daten von natürlichen Personen sind alle Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen und so mit einem Menschen direkt oder indirekt in Verbindung gebracht werden können.

R

Recht auf Berichtigung

Menschen haben das Recht darauf, dass falsche oder unvollständige personenbezogene Daten berichtigt bzw. ergänzt werden.

Recht auf Vergessenwerden/Löschung

Menschen haben das Recht, dass ihre nicht mehr für den Verarbeitungszweck notwendigen und nicht mehr genutzten personenbezogenen Daten aktiv gelöscht werden, sobald alle Formalitäten abgewickelt und die gesetzlichen Aufbewahrungsfristen abgelaufen sind.

S

Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie für die Zwecke, für die sie verarbeitet wurden, erforderlich sind. Wenn dieser Zweck wegfällt, müssen die Daten gelöscht werden.

V

*Verantwortliche Stelle/Verantwortliche*r*

Eine natürliche oder juristische Person, kirchliche Stelle im Sinne von Art. 2 Nr. 1 des DSG-EKD oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verschlüsselung

Im Bereich der Datenübertragung wird die Umwandlung von Daten von einem lesbaren Format in ein verschlüsseltes Format, das erst nach einer Entschlüsselung wieder gelesen oder verarbeitet werden kann, als Verschlüsselung bezeichnet. Im Datenschutz ist dies eine grundlegende Methode, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen.

Verstoß

Im Datenschutzrecht liegt ein Verstoß gegen das Datenschutzrecht – und damit die Verletzung des Schutzes personenbezogener Daten – vor, wenn absichtlich oder unabsichtlich personenbezogene Daten unrechtmäßig vernichtet, verändert, veröffentlicht, weitergegeben, gespeichert oder sonst auf irgendeine Weise verarbeitet werden oder verloren gehen.

Verzeichnis von Verarbeitungstätigkeiten

Ein Verzeichnis von Verarbeitungstätigkeiten ist ein schriftliches oder elektronisches, internes Verzeichnis, in welchem der Umgang eines Vereins oder Verbands mit personenbezogenen Daten dargestellt wird.

W

Widerruf

Eine betroffene Person hat grundsätzlich das Recht, ihre Einwilligung zur Datenverarbeitung zu widerrufen. Wenn die Grundlage einer Daten-

vereinbarung rein auf dem Erlaubnisvorbehalt der »Einwilligung« beruht, müssen die Daten somit gelöscht werden. Dabei hat ein Widerruf erst mit Blick auf zukünftige, verarbeitende Tätigkeiten Bestand. Die Datenverarbeitung bis zum Zeitpunkt des Widerrufs bleibt rechtmäßig.

Widerspruch

Eine betroffene Person hat das Recht, Widerspruch aus Gründen, die sich aus ihrer »besonderen Situation« ergeben, gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen. Ein Widerspruch verpflichtet den Verband/Verein dazu, die Verarbeitung zu unterlassen, soweit kein zwingendes kirchliches Interesse besteht, das Interesse einer dritten Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Z

Zweckbindung

Es muss ein eindeutiger Zweck für die Verarbeitung personenbezogener Daten durch einen Verband/Verein vorliegen. Für zusätzliche oder neue Nutzungszwecke von bereits erhobenen Daten bedarf es der expliziten Zustimmung zur Verarbeitung durch die betroffenen Personen.

Quellenverzeichnis

Bundesnetzagentur (2020): Pressemitteilung: Bundesnetzagentur veröffentlicht Bericht zu Online-Kommunikationsdiensten. *www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2020/20200522_OTT.html* (abgerufen am 12.01.2021).

Der Beauftragte für den Datenschutz der EKD (2018a): Merkblatt für den Datenschutz für Ehrenamtliche. *https://datenschutz.ekd.de/infothek-items/verpflichtungserklaerung-von-ehrenamtlich-mitarbeitenden-auf-das-datengeheimnis/* (abgerufen am 17.11.2020).

Der Beauftragte für den Datenschutz der EKD (2018b): Ergänzende Stellungnahme des Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland und des Beauftragten für den Datenschutz der Nordkirche zum Einsatz von Messenger-Diensten. In: Stellungnahme 002–2018. *https://datenschutz.ekd.de/wp-content/uploads/2018/10/Erg %C3 %A4nzende-Stellungnahm-Messgr-Dienste.pdf* (abgerufen am 25.11.2020).

Evangelische Kirche in Hessen und Nassau (2021): FAQs zum Datenschutz. *https://unsere.ekhn.de/medien/datenschutz/haeufig-gestellte-fragen-faq.html* (abgerufen am 24.02.2021).

Kamm, K. (2020): Rechtliche Prüfungsergebnisse und Rechtsgutachten eingeholt vom örtlich Beauftragten für den Datenschutz des VCP. Kremer Rechtsanwälte. Köln.

Reichmann, S. (2018): Los geht's. Datenschutz in der Jugendarbeit. Landesjugendring Niedersachsen (Hrsg.). Hannover.

Schrock, T. (2018): DSGVO-Artikelserie. Teil 1–3. Deutscher Bundesjugendring (Hrsg.). *https://tooldoku.dbjr.de/2018/05/dsgvo-artikelserie-1-diedatenschutzgrundverordnu ng-worum-gehts/* (abgerufen am 24.11.2020).

Verbraucherzentrale NRW e.V. (2021): Datenschutzrecht – wichtige Begriffe zum Datenschutz erklärt. *www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/datenschutzrecht-wichtige-begriffe-zum-datenschutz-erklaert-55 444* (abgerufen am 25.02.2021).

Weller, F. (2020): Datenschutz für Vereine. Leitfaden für die Vereinspraxis. Erich Schmidt Verlag (Hrsg.). Berlin.

Kontakt

VCP e.V.
Wichernweg 3
34121 Kassel
0561 784 370
info@vcp.de
www.vcp.de

Impressum

Herausgegeben von der*vom örtlich Beauftragten für den Datenschutz des VCP

Verantwortliches Mitglied im Vorstand:
Natascha Sonnenberg

Redaktion: Lena Dohmann, Lena Kiefer, Tobias Schwick

Layout: FOLIANT-Editionen, Ralf Tempel
info@foliant-editionen.de

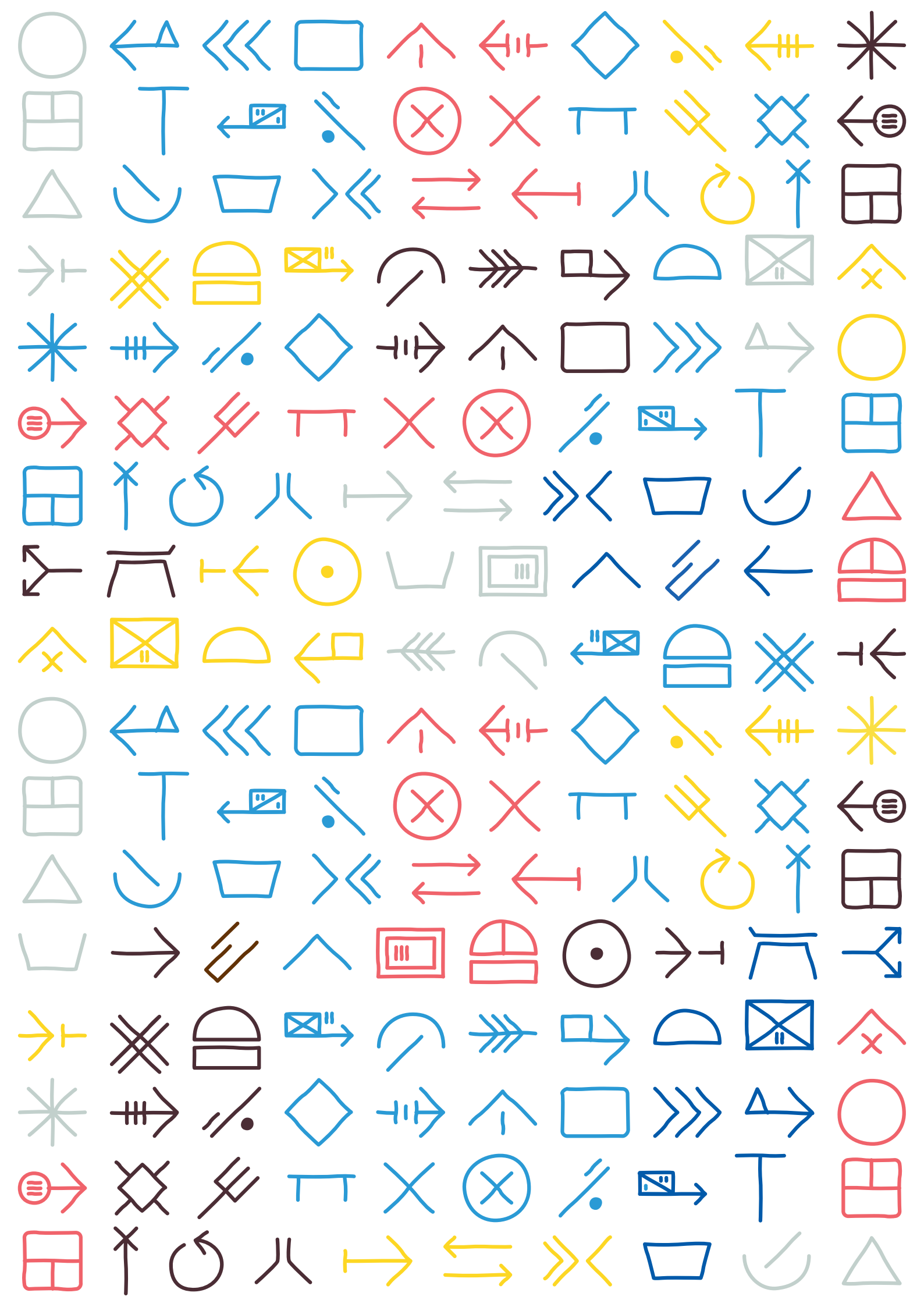
Stand: März 2021

Der VCP ist Mitglied im Ring Deutscher Pfadfinderinnenverbände (RDP) und im Ring deutscher Pfadfinderverbände (RdP) und über diese im Weltbund der Pfadfinderinnen (WAGGGS) und in der Weltorganisation der Pfadfinderbewegung (WOSM). Darüber hinaus ist der VCP Mitglied im Deutschen Bundesjugendring (DBJR) und in der Arbeitsgemeinschaft der Evangelischen Jugend in Deutschland e. V. (aej).

Wir danken für die freundliche Unterstützung und Förderung unserer Arbeit.

Bundesministerium für Familie, Senioren, Frauen und Jugend

EKD Evangelische Kirche in Deutschland



vcp

VERBAND CHRISTLICHER
PFADFINDERINNEN UND
PFADFINDER

WORLD ASSOCIATION
OF GIRL GUIDES
AND GIRL SCOUTS

SCOUTS
Creating a Better World